INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE FÍSICA Y MATEMÁTICAS

Fracciones continuas y algunas de sus aplicaciones

T E S I S

QUE PARA OBTENER EL TÍTULO DE
LICENCIADO EN FÍSICA Y MATEMÁTICAS

PRESENTA

ANTONIO MIGUEL MENDOZA

Director de Tesis:
Abelardo Santaella Quintas

México, D.F. Septiembre de 2006

Agradecimientos

En primer lugar le doy gracias a la vida, por permitirme existir.

Agradezco de manera muy especial a mis padres, Carlota Mendoza Cruz y Francisco Miguel López, quienes con su cuidado y ejemplos de buenos padres, hicieron de mí una buena persona, por brindarme su confianza y apoyarme siempre, pues sin ellos habría sido muy difícil lograr ser lo que soy. Gracias, por la dignidad que me enseñaron. Así como a mis hermanas y hermanos, por estar a mi lado motivandome en todo momento a salir adelante, por tenderme la mano ante las adversidades y por ser parte de mí. Gracias, por permitirme creer que puedo ser.

Agradezco al maestro Abelardo Santaella Quintas, quien fue paciente al asesorarme de principio a fin en el desarrollo de cada uno de los temas del presente trabajo.

También a mis sinodales el Lic. Manuel Robles Bernal, M. en C. Andrés S. Díaz Castro, Dr. Pablo Lam Estrada, Dra. Martha Rzedowski Calderón, quienes dedicaron parte de su valioso tiempo a la revisión de este trabajo, pues sus observaciones hechas fueron de gran utilidad para la culminación del mismo.

Y gracias a tí amigo lector por interesarte en leer este trabajo, espero te pueda servir de ayuda.

Notación.

Simbolo	
$\mathbb{N}$	Naturales
$\mathbb{Z}$	Enteros
$\mathbb{Q}$	Racionales
$\mathbb{R}$	Reales
$\mathbb{C}$	Complejos
$\mathbb{F}$	Campo
$\mathbb{N}_0$	$\mathbb{N} \cup \{0\}$
$\mathbb{R}^*$	$\mathbb{R} - \{0\}$
$\mathbb{C}^*$	$\mathbb{C} - \{0\}$
$[\![\ ]\!]$	Función parte entera

Índice general

Agradecimientos **2**

1. Introducción **5**

2. Fracciones continuas **13**
2.1. Fracciones continuas 13
2.2. Desarrollos de irracionales cuadráticos 26
2.3. Transformaciones modulares 30

3. Aplicaciones de las fracciones continuas **34**
3.1. Ecuación diofantina de primer grado. 34
3.2. La fracción continua de e 42

4. Unidades de campos cuadráticos **58**
4.1. Conceptos básicos 58
4.2. Números algebraicos 64
4.3. Campos de números algebraicos 66
4.4. Unidades en campos cuadráticos 71

Conclusiones **81**

Bibliografía **83**

Capítulo 1

Introducción

El algoritmo euclidiano para encontrar el máximo común divisor de dos enteros conduce de manera inmediata a un método importante para representar el cociente de dos enteros como una fracción compuesta.

Aplicado a los números 840 y 611, por ejemplo el algoritmo euclidiano produce la serie de ecuaciones:

$$840 = 1 \cdot 611 + 229 \qquad 611 = 2 \cdot 229 + 153$$

$$229 = 1 \cdot 153 + 76 \qquad 153 = 2 \cdot 76 + 1$$

así $(820, 611) = 1$. De estas ecuaciones podemos obtener las siguientes expresiones:

$$\frac{840}{611} = 1 + \frac{229}{611} = 1 + \frac{1}{611/229}$$

$$\frac{611}{229} = 2 + \frac{153}{229} = 2 + \frac{1}{229/153}$$

$$\frac{229}{153} = 1 + \frac{76}{153} = 1 + \frac{1}{153/76}$$

$$\frac{153}{76} = 2 + \frac{1}{76}$$

Al combinar estas ecuaciones obtenemos el desarrollo del número racional 840/611 en la forma

$$\frac{840}{611} = 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{76}}}}$$

la expresión anterior se denomina *fracción continua*,[1] el algoritmo euclidiano nos da un método para expresar cualquier número racional en esta forma.

Como antecedentes históricos podemos mencionar que los egipcios emplearon por primera vez las fracciones, pero sólo como divisores de la unidad $(1/n)$. Con lo cual surgen las primeras operaciones de carácter aditivo para enteros y fracciones, además esto permite hallar soluciones a ecuaciones de la forma $ax = b$. A su vez la civilización mesopotámica desarrolló un eficaz sistema de notación fraccionaria que permitió establecer aproximaciones decimales sorprendentes, su capacidad de abstracción fue tal que desarrollaron muchas de las que hoy se conocen como ecuaciones diofantinas. Una contribución algebraica importante de la antigua civilización china fue el establecer un método genérico de resolución de sistemas de ecuaciones lineales muy similar al que hoy conocemos como método de Gauss. La característica principal del desarrollo matemático en la civilización india es el predominio de las reglas aritméticas de cálculo, introducen al cero, números negativos y aceptan como válidos a los números irracionales. Obtienen reglas de resolución de ecuaciones lineales y cuadráticas. Desarrollaron también métodos de resolución de ecuaciones diofantinas, llegando incluso a plantear y resolver (siglo XII) la ecuación de Pell $x^2 - dy^2 = 1$.

En la época helénica los problemas prácticos relacionados con las necesidades de cálculo aritmético se desprendieron de una rama denominada logística a la cual se le atribuyó entre otras operaciones, el cálculo con fracciones. Se descubrió de manera tajante la irracionalidad, demostrando por ejemplo la irracionalidad de $\sqrt{2}$. En la época del dominio romano destacan los métodos de Diofanto que encontró soluciones a más de 50 clases diferentes de ecuaciones generalmente de segundo grado, denominadas ecuaciones diofantinas. En resumen, la matemática de la antigua Grecia representa uno de los primeros establecimientos de las matemáticas como ciencia, desarrolándose en

[1] de la mayor importancia en una rama de la aritmética avanzada conocida como análisis diofantino.

su seno dentro de ciertos límites los elementos de las ciencias matemáticas ulteriores: álgebra, análisis infinitesimal, geometría analítica, mecánica teórica y el método axiomático. En el imperio musulmán, a partir de la segunda mitad del siglo $VIII$, se desarrollaron un gran número de procedimientos de cálculo y algoritmos especiales, entre ellos: la obtención del número π con 17 cifras exactas (después de más de 150 años, en 1593, en Europa, Viete encontró sólo 9 cifras exactas), también se analizó la extracción aproximada de raíces por interpolación. En el continente europeo, las matemáticas alcanzaron éxitos notorios sólo en la época del medievo desarrollado y especialmente en el renacimiento. Uno de los primeros centros de enceñanza fue organizado en Reims (Francia). Durante el siglo $XIII$ surgió la figura de Leonardo de Pisa $(1180-1250)$ más conocido como Fibonacci, quien quedó inmortalizado por la famosa sucesión de Fibonacci. A comienzos del siglo $XVIII$, en 1707, vió la luz la aritmética de Newton. En ella el álgebra se exponía en estrecha relación con el desarrollo de los métodos de cálculo. Después de la aritmética de Newton surgieron una serie de monografías, especialmente centradas en el procedimento de resolución numérica de ecuaciones elaboradas por Halley, Lagrange, Fourier y Maclaurin, entre otros. En 1768, apareció la aritmética universal de Euler. En ella se analizan varios resultados, entre ellos: se aclaran las operaciones con números, monomios, radicales y complejos, se introducen las series como medio de expresión de las funciones racionales fraccionarias, se introducen también las proporciones y progresiones, las fracciones decimales periódicas y se estudian los métodos de resolución de ecuaciones algebraicas. Fue también Euler quien se ocupó de una manera definitiva de lo que hoy conocemos como teoría de números, a él también debemos la actual teoría de congruencias. De igual importancia que la teoría de congruencias, fueron sus trabajos sobre problemas de análisis diofántico, para cuyas necesidades elaboró y fundamentó la teoría de las fracciones continuas. La teoría de números en el siglo $XVIII$, se convirtió pues en una rama independiente sintetizada en los trabajos de Euler, Lagrange, Legendre y Jean D′Alembert entre otros. El siglo XIX merece ser más que ningún otro periodo anterior, la edad de oro de las matemáticas. Las particularidades del nuevo periodo se manifiestan ya nada más al comenzar el siglo. En álgebra hay que tener en cuenta los trabajos de Gauss, Abel y Galois sobre la resolución de ecuaciones algebraicas en radicales. En esta época se introdujeron una serie de conceptos, entre ellos el de grupo, que yace en la base del álgebra moderna. Pasó medio siglo desde los trabajos de Gauss, Abel y Galois y el centro de atención en las investigaciones algebraicas se transladó a la teoría de grupos, anillos, estructuras.

En álgebra comenzó el periodo de las matemáticas modernas. En el año 1872 surgieron una serie de trabajos, escritos por Cantor, Dedekind, Weierstrass, Heine y Meray, cuyo único objetivo era el de dotar de una teoría rigurosa al número real. Así Dedekind definió el número real como una cortadura en el conjunto de los números racionales, dando al conjunto de números reales una interpretación geométrica en forma de línea recta. Cantor por su parte identificó al número real con una sucesión convergente de números racionales, y entre los años 1879 a 1884 introdujo entre otros el concepto de punto límite. Quizás no haya otro ejemplo de influencia, a la vez decisiva y desdichada, de los acontecimientos públicos y privados de una vida sobre la propia actividad creadora, que en el caso de Evariste Galois, quien entre 1829 y 1830 hace conocer sus primeros trabajos sobre teoría de las ecuaciones, teoría de números, cuestiones de análisis y sobre fracciones continuas.

Ocurren procesos de límite interesantes en relación con las fracciones continuas. Una fracción continua finita, tal como

$$x = \frac{67}{29} = 2 + \cfrac{1}{3 + \cfrac{1}{4 + \cfrac{1}{2}}} = [2, 3, 4, 2]$$

representa a un número racional. Se prueba sin dificultad que cualquier racional admite una representación como fracción continua finita utilizando el algoritmo de Euclides. Para los irracionales, empero, el algoritmo no termina después de un número finito de pasos. Lleva en cambio a una sucesión de fracciones de longitud creciente, cada una representando un número racional. En particular todos los números algebraicos reales de grado 2 (raíces de un polinomio irreducible de grado 2) pueden expresarse de esta manera. Consideremos, por ejemplo, el número $x = \sqrt{2} - 1$, que es una raíz de la ecuación cuadrática

$$x^2 + 2x = 1 \quad \text{o} \quad x = \frac{1}{2 + x}$$

si sustituimos a x nuevamente por $1/(2 + x)$ en el segundo miembro, esto da la expresión

$$x = \cfrac{1}{2 + \cfrac{1}{2 + x}}, \quad \text{y luego} \quad x = \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + x}}}$$

sin dificultad, observamos que este proceso se aplica sucesivamente (n pasos), conforme n tiende a infinito, obtenemos la fracción continua infinita

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \ddots}}}}$$

Esta fórmula notable relaciona a $\sqrt{2}$ con los enteros de un modo más impresionante que la expresión decimal de $\sqrt{2}$, la cual no presenta ninguna regularidad en la sucesión de sus dígitos.

Para la raíz positiva de cualquier ecuación cuadrática de la forma

$$x^2 = ax + 1 \quad \text{o} \quad x = a + \frac{1}{x}$$

obtenemos la expansión

$$x = a + \cfrac{1}{a + \cfrac{1}{a + \cfrac{1}{a + \cfrac{1}{a + \ddots}}}}$$

las fracción continua anterior, puede expresarse utilizando la siguiente notación $[a, a, a, \ldots]$, la cual entonces corresponde a la raíz (positiva) de una ecuación de la forma $x^2 - ax - 1 = 0$. Por ejemplo, tomando $a = 1$, encontramos

$$x = \frac{1+\sqrt{5}}{2} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \ddots}}}}$$

donde denotamos al número anterior por ϕ, es decir $\phi = \dfrac{1+\sqrt{5}}{2}$ conocido como número áureo, la raíz positiva de la ecuación $x^2 - x - 1$, y posee la expresión más simple como fracción continua, a saber: $\phi = [1, 1, 1, \ldots]$, sin embargo esta fracción continua es la que converge más lentamente, sus convergentes sucesivos son: $1, 2, 3/2, 5/3, 8/5, \ldots$ que son precisamente los cocientes de dos términos cosecutivos de la conocida sucesión de Fibonacci $\{1, 1, 2, 3, 5, 8, 13, \ldots\}$, luego el cociente de dos términos consecutivos de la sucesión de Fibonacci aproximan al número ϕ tanto como se desee.

Estos ejemplos son casos especiales de un teorema general que establece que las raíces reales de ecuaciones cuadráticas con coeficientes enteros tienen desarrollos periódicos en fracciones continuas, tal y como los números racionales tienen expansiones decimales periódicas.

Euler fue capaz de encontrar fracciones continuas infinitas casi igual de sencillas para e y π, siendo estas las siguientes

$$e = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{6 + \ddots}}}}}}}}$$

$$\pi = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{292 + \cfrac{1}{1 + \cfrac{1}{1 + \ddots}}}}}}$$

$$\frac{\pi}{4} = \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{15 + \ddots}}}}}}$$

El campo de aplicaciones de las fracciones continuas es muy amplio, podemos mencionar por ejemplo su utilidad en las aproximaciones diofantinas (aproximaciones de números reales por racionales), sucesiones recurrentes, razón aurea, ecuaciones diofantinas, pruebas de primalidad y métodos de factorización, relaciones de congruencias, etc.

En el presente trabajo abordaremos algunas de las aplicaciones de las fracciones continuas. En el Capítulo 2 introducimos algunos conceptos y resultados básicos referentes al tema. Entre los resultados que posteriomente tendrán una aplicación importante tenemos, que los números que poseen un desarrollo periódico como fracción continua corresponden a raíces de polinomios de segundo grado con coeficientes enteros y recíprocamente. Otro de los resultados importantes corresponde a afirmar que los números irracionales (en general reales) tienen una única representación como fracción continua.

La teoría desarrollada nos permitirá en el Capítulo 3, analizar un método de solución aplicable a ecuaciones diofantinas lineales en dos variables, obtendremos además la representación como fracción continua del número e. El desarrollo en fracción continua de números irracionales de la forma $\sqrt{d}$, con d libre de cuadrado, surge de la necesidad de obtener un método de solución de la ecuación de Pell, que es la ecuación diofantina $x^2 - dy^2 = 1, x, y$ positivos,

de la cual toda solución es un convergente de la fracción continua de $\sqrt{d}$. Si (p, q) es la solución entera más pequeña de la ecuación de Pell, entonces todas sus soluciones son dadas por $(p + q\sqrt{d})^n = p_n + q_n\sqrt{d}$. Esto nos lleva a pensar en unidades de campos cuadráticos, por lo que en el capítulo final, introduciremos algunos conceptos y resultados básicos de la teoría de anillos y campos numéricos, y finalizaremos calculando unidades de campos cuadráticos.

Capítulo 2

Fracciones continuas

En este capítulo desarrollamos parte de la teoría básica, sobre fracciones continuas.

2.1. Fracciones continuas

Definición 2.1

(i) Una fracción continua finita es una expresión de la forma

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}$$

donde cada $a_i \in \mathbb{R}$ y $a_i > 0$ para $1 \leq i \leq n$. Utilizaremos la notación $[a_0, \ldots, a_n]$ para denotar a la expresión anterior.

(ii) $[a_0, \ldots, a_n]$ es llamada una fracción continua simple si $a_0, \ldots, a_n \in \mathbb{Z}$.

(iii) La fracción continua $C_k = [a_0, \ldots . a_k]$, $0 \leq k \leq n$, es llamado el k-ésimo convergente de $[a_0, \ldots, a_n]$.

Evidentemente una fracción continua simple finita representa un número racional. Recíprocamente, usando el algoritmo euclidiano, uno puede mostrar que cada número racional puede expresarse como una fracción continua simple finita.

Adecuando la notación podemos considerar las siguientes igualdades

$$x_0 = a_n \qquad\qquad x_{i+1} = a_{n-1-i} + \frac{1}{x_i}, \quad i \in \mathbb{N}_0$$

las cuales determinan una definición formal por recurrencia de derecha a izquierda.

Considere C_k como antes, así :

$$C_n = [a_0, \ldots, a_n] = \frac{p_n}{q_n}$$

donde $p_n, q_n \in \mathbb{R}$, convenimos en que si $a_0 = 0$, entonces $p_0 = 0$, y $q_0 = 1$.

Teorema 2.1 *Considere la fracción continua* $[a_0, \ldots, a_n]$. *Defina la sucesión* $p_0, \ldots, p_n$ *y* $q_o, \ldots, q_n$ *recursivamente como sigue:*

$$p_0 = a_0 \qquad\qquad q_0 = 1$$

$$p_1 = a_1 a_0 + 1 \qquad\qquad q_1 = a_1$$

$$p_k = a_k p_{k-1} + p_{k-2} \qquad\qquad q_k = a_k q_{k-1} + q_{k-2}$$

para $k \geq 2$. *Entonces el* k*-ésimo convergente satisface que* $C_k = \dfrac{p_k}{q_k}$.

Demostración: Aplicando inducción sobre k. Para $k = 0$, tenemos que $C_0 = a_0 = \dfrac{p_0}{q_0}$, sea ahora $k = 1$, entonces

$$C_1 = [a_0, a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} = \frac{p_1}{q_1}.$$

Para $k \geq 1$, supongamos válido

$$C_k = \frac{p_k}{q_k} = \frac{a_k p_{k-1} + p_{k-2}}{a_k q_{k-1} + q_{k-2}}$$

donde se tiene que $p_{k-1}, p_{k-2}, q_{k-1}, q_{k-2}$ dependen únicamente de $a_0, a_1, \ldots a_{k-1}$. Resta probar para $k+1$, así

$$C_{k+1} = \left[a_0, a_1, \ldots, a_{k-1}, a_k + \frac{1}{a_{k+1}}\right]$$

$$= \frac{\left(a_k + \dfrac{1}{a_{k+1}}\right) p_{k-1} + p_{k-2}}{\left(a_k + \dfrac{1}{a_{k+1}}\right) q_{k-1} + q_{k-2}}$$

$$= \frac{a_{k+1}(a_k p_{k-1} + p_{k-2}) + p_{k-1}}{a_{k+1}(a_k q_{k-1} + q_{k-2}) + q_{k-1}}$$

$$= \frac{a_{k+1}p_k + p_{k-1}}{a_{k+1}q_k + q_{k-1}} = \frac{p_{k+1}}{q_{k+1}}.$$

■

Del teorema anterior se obtiene que la sucesión $\{q_n\}_{n\geq 0}$ es creciente, y si $a_0 > 0$ entonces $\{p_n\}_{n\geq 0}$ también lo es. Tenemos además la siguiente consecuencia simple:

Teorema 2.2 *Con la notación anterior, se cumple:*

$$(i) \quad p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1} \qquad \text{para } 1 \leq k$$

$$(ii) \quad C_k - C_{k+1} = \frac{(-1)^{k+1}}{q_k q_{k+1}} \qquad \text{para } 1 \leq k \leq n$$

$$(iii) \quad C_k - C_{k-2} = \frac{a_k(-1)^k}{q_k q_{k-2}} \qquad \text{para } 2 \leq k \leq n$$

Demostración: Procedamos por inducción sobre k.

(i) Para $k = 1$, obtenemos

$$p_1q_0 - p_0q_1 = (a_0a_1 + 1) \cdot 1 - a_0a_1 = 1 = (-1)^{1-1}$$

Para $k = 2$, obtenemos

$$p_2q_1 - p_1q_2 = (a_2p_1 + p_0)q_1 - p_1(a_2q_1 + q_0) = -(p_1q_0 - p_0q_1) = -1$$

Supongamos válido el resultado para $k \geq 1$, resta probar para $k + 1$, entonces:

$$p_{k+1}q_k - p_kq_{k+1} = (a_{k+1}p_k + p_{k-1})q_k - p_k(a_{k+1}q_k + q_{k-1})$$

$$= p_{k-1}q_k - p_kq_{k-1} = -(-1)^{k-1} = (-1)^k.$$

(ii) De (i)

$$p_kq_{k+1} - q_kp_{k+1} = (-1)^{k+1}$$

dividiendo por q_kq_{k+1} la expresión anterior, obtenemos fácilmente la identidad requerida.

(iii) Ahora

$$C_k - C_{k-2} = \frac{p_k}{q_k} - \frac{p_{k-2}}{q_{k-2}} = \frac{p_kq_{k-2} - p_{k-2}q_k}{q_kq_{k-2}}$$

Pero

$$p_kq_{k-2} - p_{k-2}q_k = (a_kp_{k-1} + p_{k-2})q_{k-2} - p_{k-2}(a_kq_{k-1} + q_{k-2})$$

$$= a_k(p_{k-1}q_{k-2} - p_{k-2}q_{k-1}) = a_k(-1)^{k-2} = a_k(-1)^k$$

estableciendo así la identidad requerida. ■

De la parte (i) del teorema anterior, podemos concluir que si $[a_0, \ldots, a_n]$ es una fracción continua simple, entonces los enteros p_k y q_k son primos relativos.

El Teorema 2.2 nos proporciona la información acerca de cómo varían los convergentes C_k cuando k crece. En efecto, de (iii):

$$C_k - C_{k-2} = \frac{a_k(-1)^k}{q_k q_{k-2}}$$

así $C_k > C_{k-2}$ para k par y $C_k < C_{k-2}$ si k es impar, además

$$C_{2l} - C_{2l+1} = \frac{(-1)^{2l+1}}{q_{2l} q_{2l-1}} < 0$$

obtenemos así que $C_{2l-1} > C_{2l}$, de esto

$$C_{2k} < C_{2(j+k+1)} < C_{2(j+k)+1} < C_{2j+1}$$

con $j \geq 0$ y $k \geq 0$. Obtenemos así

$$C_0 < C_2 < C_4 < \ldots < C_5 < C_3 < C_1$$

Del análisis anterior se concluye que la sucesión de convergentes, con índices pares es creciente mientras que la sucesión de convergentes con índices impares es decreciente, más aún que todo convergente de índice par es menor que cualquiera con índice impar.

Estamos en condiciones de probar la convergencia de las fracciones continuas.

Teorema 2.3 *Sea $\{a_i\}_{i\geq 0}$ una sucesión infinita de enteros con $a_i > 0$ para $i \geq 1$ y sea $C_k = [a_0, \ldots, a_k]$. Entonces la sucesión $\{C_k\}_{k\geq 0}$ es convergente.*

Demostración: Como demostramos anteriormente, los convergentes están ordenados como se indica

$$C_0 < C_2 < C_4 < \ldots < C_5 < C_3 < C_1$$

Luego $C_1 > C_3 > C_5 > \ldots$, donde cada $C_{2j+1} > C_0$, así la sucesión $\{C_{2j+1}\}_{j\geq 0}$ es decreciente y acotada inferiormente, por lo tanto convergente, sea

$$\lim_{j\to\infty} C_{2j+1} = \alpha_1.$$

Además $C_0 < C_2 < C_4 < \ldots$ y $C_{2j} < C_{2k+1}$ para todo $j, k \geq 0$. En particular, cada $C_{2j} < C_1$, entonces la sucesión $\{C_{2j}\}_{j\geq 0}$ es creciente y acotada superiormente, por lo tanto también es convergente, consideremos

$$\lim_{j\to\infty} C_{2j} = \alpha_2.$$

Por demostrar que $\alpha_1 = \alpha_2$. Como cada $a_i \geq 1$ para $i \geq 1$ y $q_0, q_1 \geq 1$, se prueba fácilmente por inducción sobre k que

$$q_k = a_k q_{k-1} + q_{k-2} \geq 2k - 3$$

Aplicando (ii) del Teorema 2.2, obtenemos

$$C_{2j+1} - C_{2j} = \frac{1}{q_{2j+1}q_{2j}} \leq \frac{1}{(4j-1)(4j-3)} \underset{j\to\infty}{\longrightarrow} 0$$

Así ambas sucesiones convergen al mismo límite, así $\alpha = \alpha_1 = \alpha_2$, y

$$\lim_{j\to\infty} C_j = \alpha.$$

■

Definición 2.2 *La fracción continua $[a_0, a_1, \ldots]$, se define como el límite de la sucesión de convergentes $\{C_k\}_{k\geq 0}$ cuando $k \to \infty$, es decir;*

$$[a_0, a_1, \ldots] = \lim_{k\to\infty} C_k.$$

Proposición 1 *Sea $\alpha = \alpha_0$ un número irracional mayor que cero. Definimos la sucesión $\{a_i\}_{i\in\mathbb{N}_0}$ recursivamente como sigue*

$$a_k = [\![\ \alpha_k\ ]\!] \qquad\qquad \alpha_{k+1} = \frac{1}{\alpha_k - a_k}.$$

Entonces $\alpha = [a_0, a_1, \ldots]$ es la representación de α como una fracción continua simple.

Demostración: Procedamos por inducción sobre k, se verifica fácilmente que cada α_k es irracional. Claramente para $k \geq 1$ $\alpha_k > 1$ así cada $a_{k+1} \geq 1$, luego $[a_0, a_1, \ldots]$ es una fracción continua simple. Entonces

$$\alpha = \alpha_0 = [\![\ \alpha_0\ ]\!] + (a_0 - [\![\ \alpha_0\ ]\!]) = a_0 + \frac{1}{\alpha_1}$$

$$= [a_0, \alpha_1] = [a_0, a_1, \alpha_2] = \cdots = [a_0, a_1, \ldots, a_k, \alpha_{k+1}]$$

para toda k. Por el Teorema 2.1, obtenemos

$$\alpha = \frac{\alpha_{k+1}p_k + p_{k-1}}{\alpha_{k+1}q_k + q_{k-1}}$$

así que

$$|\alpha - C_k| = \left|\frac{\alpha_{k+1}p_k + p_{k-1}}{\alpha_{k+1}q_k + q_{k-1}} - \frac{p_k}{q_k}\right| = \left|\frac{-(p_kq_{k-1} - p_{k-1}q_k)}{(\alpha_{k+1}q_k + q_{k-1})q_k}\right|$$

$$= \left|\frac{1}{(\alpha_{k+1}q_k + q_{k-1})q_k}\right| < \frac{1}{q_k^2} \leq \frac{1}{(2k-3)^2} \underset{k\to\infty}{\longrightarrow} 0$$

Así

$$\alpha = \lim_{k\to\infty} C_k = [a_0, a_1, \ldots].$$

■

Evidentemente de lo anterior concluimos que cada número real α tiene una representación como fracción continua simple. Más aún podemos demostrar que para el caso de un número irracional su representación como fracción continua simple es única.

Teorema 2.4

(a) Sea α un número irracional y $C_j = \dfrac{p_j}{q_j}$, para $j \in \mathbb{N}$, el convergente de una fracción continua simple de α. Si $r, s \in \mathbb{Z}$ con $s > 0$ y k es un entero positivo tal que

$$|s\alpha - r| < |q_k\alpha - p_k|$$

entonces $s \geq q_{k+1}$.

(b) Si α es un número irracional y $\dfrac{r}{s}$ es un número racional con $s > 0$ tal que

$$\left|\alpha - \frac{r}{s}\right| < \frac{1}{2s^2}$$

Entonces $\dfrac{r}{s}$ es un convergente de la fracción continua de α.

Demostración:

(a) Procedamos por contradicción, supongamos así que $1 \leq s < q_{k+1}$. Para cada $k \geq 0$ consideremos el sistema de ecuaciones lineales

$$p_k x + p_{k+1} y = r$$

$$q_k x + q_{k+1} y = s$$

Utilizando eliminación gaussiana obtenemos:

$$(p_k q_{k+1} - p_{k+1} q_k)x = r q_{k+1} - s p_{k+1}$$

$$(p_{k+1} q_k - p_k q_{k+1})y = r q_k - s p_k$$

Aplicando el Teorema 2.2 parte (i), obtenemos $p_k q_{k+1} - p_{k+1} q_k = (-1)^{k+1}$, por lo que la solución del sistema es única y está dada por

$$x = (-1)^k(sp_{k+1} - rq_{k+1})$$

$$y = (-1)^k(rq_k - sp_k).$$

Probaremos que x e y son no nulos y tienen distinta paridad (signo). Supongamos que $x = 0$, entonces

$$\frac{r}{s} = \frac{p_{k+1}}{q_{k+1}}.$$

Puesto que $(p_{k+1}, q_{k+1}) = 1$, esto implica que $q_{k+1}|s$, así $q_{k+1} \leq s$ lo cual es una contadicción. Supongamos ahora $y = 0$, entonces $r = p_k x, s = q_k x$, entonces

$$|s\alpha - r| = |x| \cdot |q_k\alpha - p_k| \geq |q_k\alpha - p_k|$$

lo cual es una contradicción, luego x e y son ambos no nulos.

Supongamos ahora que $y < 0$. Como $q_k x = s - q_{k+1}y$ con $q_j \geq 0$, tenemos $x > 0$. Si $y > 0$, entonces $q_{k+1}y \geq q_{k+1} > s$, tenemos $q_k x = s - q_{k+1}y < 0$, luego $x < 0$.

Por otra parte si k es par, tenemos la siguiente condición

$$\frac{p_k}{q_k} < \alpha < \frac{p_{k+1}}{q_{k+1}}$$

mientras que si k es impar se tiene

$$\frac{p_{k+1}}{q_{k+1}} < \alpha < \frac{p_k}{q_k}$$

En cada caso obtenemos que $q_k\alpha - p_k$ y $q_{k+1}\alpha - p_{k+1}$ tienen signos opuestos, luego $x(q_k\alpha - p_k)$ e $y(q_{k+1}\alpha - p_{k+1})$ tienen el mismo signo, entonces

$$|s\alpha - r| = |(q_k x + q_{k+1} y)\alpha - (p_k x + p_{k+1} y)|$$

$$= |x(q_k\alpha - p_k) + y(q_{k+1}\alpha - p_{k+1})|$$

$$= |x||q_k\alpha - p_k| + |y||q_{k+1}\alpha - p_{k+1}|$$

$$\geq |x||q_k\alpha - p_k| \geq |q_k\alpha - p_k|$$

lo cual es una contradicción, obtenemos así que $s \geq q_{k+1}$.

(b) Supongamos que $\frac{r}{s}$ no es convergente de la fracción continua de α, es decir $\frac{r}{s} \neq \frac{p_n}{q_n}$ para toda n. Sea k el entero no negativo más grande tal que $s \geq q_k$ (entonces $s \geq q_0 = 1$ y $q_k \to \infty$ si $k \to \infty$). Entonces $q_k \leq s < q_{k+1}$ y por (a), tenemos
$|q_k\alpha - p_k| \leq |s\alpha - r| = s\left|\alpha - \frac{r}{s}\right| < \frac{1}{2s}$, luego $\left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{2sq_k}$.

Como $\frac{r}{s} \neq \frac{p_k}{q_k}$, se tiene $|sp_k - rq_k| \geq 1$, así

$$\frac{1}{sq_k} \leq \frac{|sp_k - rq_k|}{sq_k} = \left|\frac{p_k}{q_k} - \frac{r}{s}\right| = \left|\frac{p_k}{q_k} - \frac{r}{s} + \alpha - \alpha\right|$$

$$\leq \left|\alpha - \frac{p_k}{q_k}\right| + \left|\alpha - \frac{r}{s}\right| < \frac{1}{2sq_k} + \frac{1}{2s^2}.$$

Esto implica que $\frac{1}{2sq_k} < \frac{1}{2s^2}$, así $q_k > s$, lo cual es una contradicción.

■

Se tienen los siguientes corolarios.

Corolario 2.5 *Las fracciones continuas son números irracionales.*

Demostración: Con la notación usual, supongamos que $\alpha = \dfrac{p}{q}$ con $p, q \in \mathbb{Z}$ primos relativos. Como la sucesión $\{q_n\}_{n\geq 0}$ es creciente, existe un $n \in \mathbb{N}$ tal que $q < q_{n+1}$, ahora puesto que α satiface que $C_n < \alpha < C_{n+1}$, se cumple

$$|\alpha - C_n| \leq |C_n - C_{n+1}| = \frac{1}{q_n q_{n+1}} < \frac{1}{q_n q}$$

pero por otro lado

$$|\alpha - C_n| = \left|\frac{p}{q} - \frac{p_n}{q_n}\right| = \frac{|pq_n - qp_n|}{q_n q} \geq \frac{1}{q_n q}$$

luego $\dfrac{1}{q_n q} > \dfrac{1}{q_n q}$ lo cual es absurdo, por lo tanto α es un número irracional. ■

Corolario 2.6 *Sea α un número real cualquiera, sea $\alpha = [a_0, a_1, a_2, \ldots]$ para ciertos enteros racionales, entonces el desarrollo es único.*

Demostración: Para probar la unicidad, supongamos que tenemos dos fracciones continuas tales que

$$[a_0, a_1, a_2, \ldots] = [b_0, b_1, b_2, \ldots]$$

entonces

$$a_0 \leq [a_0, a_1, a_2, \ldots] \leq a_0 + 1$$

análogamente

$$b_0 \leq [b_0, b_1, b_2, \ldots] \leq b_0 + 1$$

como el límite es irracional no se dan las igualdades, luego

$$a_0 = E([a_0, a_1, a_2, \ldots]) = E([b_0, b_1, b_2, \ldots]) = b_0$$

restando a_0 de ambos lados y tomando inversos resulta

$$[a_1, a_2, \ldots] = [b_1, b_2, \ldots]$$

repitiendo este proceso sucesivamente, se obtiene que todos los coeficientes coinciden y por tanto las fracciones continuas son iguales. ■

A continuación describiremos el procedimiento para la obtención de la fracción continua asociada a un número racional.

Sean $p, q \in \mathbb{Z}$ tales que $(p, q) = 1$, aplicando el algoritmo de la división obtenemos el siguiente sistema de ecuaciones:

$$\begin{aligned}
&p = qa_0 + r_0 && 0 < r_0 < q \\
&q = r_0a_1 + r_1 && 0 < r_1 < r_0 \\
&r_1 = r_2a_3 + r_3 && 0 < r_3 < r_2 \\
&\dots && \dots \\
&r_{n-3} = r_{n-2}a_{n-1} + r_{n-1} && 0 < r_{n-1} < r_{n-2} \\
&r_{n-2} = r_{n-1}a_n
\end{aligned} \tag{2.1.1}$$

para ciertos $r_i, a_i \in \mathbb{N}_0; i = 0, 1, \dots, n; a_0 \in \mathbb{Z}$. El algoritmo de la división garantiza que el sistema de ecuaciones anterior consta de un número finito de ecuaciones.

Luego, las expresiones del sistema (2.1.1) pueden reescribirse de la siguiente forma

$$\frac{p}{q} = a_0 + \cfrac{1}{\cfrac{q}{r_0}}$$

$$\frac{q}{r_0} = a_1 + \cfrac{1}{\cfrac{r_0}{r_1}}$$

$$\frac{r_0}{r_1} = a_2 + \cfrac{1}{\cfrac{r_1}{r_2}}$$

$$\vdots$$

$$\frac{r_{n-3}}{r_{n-2}} = a_{n-1} + \frac{1}{\frac{r_{n-2}}{r_{n-1}}}$$

$$\frac{r_{n-2}}{r_{n-1}} = a_n$$

luego, sustituyendo los valores respectivos de manera sucesiva en la primera de estas expresiones obtenemos la fracción continua asociada al número racional $\frac{p}{q}$:

$$\frac{p}{q} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}} = [a_0, \ldots, a_{n-1}, a_n] \tag{2.1.2}$$

Afirmamos que en la expresión anterior, $a_n > 1$, en efecto: supongamos que $a_n = 1$, luego de la última ecuación del sistema (2.1.1), obtenemos que $r_{n-2} = r_{n-1}$, sustituyendo en la penúltima ecuación de (2.1.1) obtenemos;

$$r_{n-3} = r_{n-2}(a_{n-1} + 1)$$

concluimos así que el algoritmo de la división termina en un paso anterior, lo cual es una contradicción. Por lo tanto $a_n > 1$.

De lo anterior se sigue que (2.1.2) puede reescribirse de la siguiente forma:

$$\frac{p}{q} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n - 1 + \cfrac{1}{1}}}}} = [a_0, \ldots, a_{n-1}, a_n - 1, 1]$$

observese que esta fracción continua tiene un coeficiente más que en (2.1.2). Así que ;

$$\frac{p}{q} = [a_0, a_1, \ldots, a_{n-1}, a_n] = [a_0, a_1, \ldots, a_{n-1}, a_n - 1, 1].$$

Del análisis anterior concluimos que los números racionales siempre poseen al menos dos representaciones en fracción continua.

Probaremos ahora un resultado que es muy útil en la manipulación de fracciones continuas.

Teorema 2.7 *Sean* $\alpha = [a_0, a_1, \ldots]$ *y* $\beta = [a_{n+1}, a_{n+2}, \ldots]$ *para* $n \geq 1$. *Entonces se cumple que:*

$$\alpha = \frac{\beta p_n + p_{n-1}}{\beta q_n + q_{n-1}}$$

Demostración: La prueba consiste simplemente en observar que en la demostración del Teorema 1.1 no se utilizo que los coeficientes a_n sean enteros, salvo para probar que $(p_n, q_n) = 1$. Por lo tanto podemos aplicarlo a $\alpha = [a_0, a_1, a_2, \ldots, a_n, \beta]$ y concluir que, aunque ahora p_{n+1} y q_{n+1} no sean números racionales

$$\alpha = \frac{p_{n+1}}{q_{n+1}} = \frac{\beta p_n + p_{n-1}}{\beta q_n + q_{n-1}}$$

■

2.2. Desarrollos de irracionales cuadráticos

Comenzamos esta sección con el siguiente resultado:

Teorema 2.8 *Sea* d *un entero positivo libre de cuadrados. Si* $|x^2 - dy^2| < \sqrt{d}$ *donde* x, y *son enteros positivos. Entonces* $\dfrac{x}{y}$ *es un convergente de la fracción continua de* $\sqrt{d}$.

Demostración: Supongamos primero que $0 < x^2 - dy^2 < \sqrt{d}$. Entonces

$$(x + \sqrt{d}y)(x - \sqrt{d}y) > 0, \text{ luego } x > \sqrt{d}y,$$

por tanto

$$\left|\sqrt{d} - \frac{x}{y}\right| = \frac{x}{y} - \sqrt{d} = \frac{x - y\sqrt{d}}{y} = \frac{x^2 - y^2 d}{y(x + y\sqrt{d})} < \frac{x^2 - y^2 d}{y(2y\sqrt{d})} < \frac{1}{2y^2}.$$

Del Teorema 2.4 inciso (b), se sigue que $\frac{x}{y}$ es convergente de la fracción continua de $\sqrt{d}$.

Consideremos ahora cuando $-\sqrt{d} < x^2 - dy^2 < 0$, tenemos

$$0 < y^2 - \frac{1}{d}x^2 < \frac{1}{\sqrt{d}}, \text{ luego } y > \frac{x}{\sqrt{d}}$$

y así

$$\left|\frac{1}{\sqrt{d}} - \frac{y}{x}\right| = \frac{y}{x} - \frac{1}{\sqrt{d}} = \frac{y - \frac{x}{\sqrt{d}}}{x} = \frac{y^2 - \frac{x^2}{d}}{x\left(y + \frac{x}{\sqrt{d}}\right)} < \frac{y^2 - \frac{x^2}{d}}{\frac{2x^2}{\sqrt{d}}} < \frac{1}{2x^2}.$$

Entonces $\frac{y}{x}$ es el convergente de la fracción continua $\frac{1}{\sqrt{d}}$. Sea α cualquier número irracional. Puesto que $\alpha = [a_0, a_1, \ldots]$, entonces $\frac{1}{\alpha} = [0, a_0, a_1, \ldots]$, tenemos que el $k+1$-ésimo convergente de la fracción continua de $\frac{1}{\alpha}$ es el recíproco del k-ésimo convergente de α para todo $k \geq 0$. Utilizando este hecho, obtenemos que $\frac{x}{y}$ es convergente de la fracción continua de $\sqrt{d}$.

■

Definición 2.3 *Una fracción continua simple es llamada periódica con periodo k si existen enteros positivos N, k tales que $a_n = a_{n+k}$ para todo $n \geq N$. Denotaremos a tal fracción continua de la siguiente manera*

$$[a_0, \ldots, a_{N-1}, \ \overline{a_N, a_{N+1}, a_{N+k-1}} \ ]$$

Teorema 2.9 *Sea α un irracional cuadrático (es decir, el polinomio mínimo del número real α sobre $\mathbb{Q}$ tiene grado 2). Entonces existen enteros P_0, Q_0, d tales que*

$$\alpha = \frac{P_0 + \sqrt{d}}{Q_0}, \quad con \;\; Q_0 | (d - P_0^2) \;\; .$$

Definimos recursivamente

$$\alpha_k = \frac{P_k + \sqrt{d}}{Q_k}$$

$$a_k = [\![\; \alpha_k \;]\!]$$

$$P_{k+1} = a_k Q_k - P_k$$

$$Q_{k+1} = \frac{d - P_{k+1}^2}{Q_k}$$

para $k = 0, 1, \ldots$, entonces $[a_0, a_1, \ldots]$ es la fracción continua simple de α.

Demostración: Existen $a, b, e, f \in \mathbb{Z}, e, f > 0$, con e libre de cuadrados, tales que

$$\alpha = \frac{a + b\sqrt{e}}{f} = \frac{af + \sqrt{eb^2 f^2}}{f^2}$$

y evidentemente $f^2 | (a^2 f^2 - eb^2 f^2)$, consideremos $P_0 = af, Q_0 = f^2, d = eb^2 f^2$. La sucesión está bien definida. Como d no es un cuadrado perfecto, tenemos $Q_k \neq 0$ para todo k. Por la Proposición 1, es suficiente probar que

$$\alpha_{k+1} = \frac{1}{\alpha_k - a_k}$$

para toda k. Entonces

$$\alpha_k - a_k = \frac{P_k + \sqrt{d}}{Q_k} - a_k = \frac{\sqrt{d} - (a_k Q_k - P_k)}{Q_k} = \frac{\sqrt{d} - P_{k+1}}{Q_k}$$

$$= \frac{d - P_{k+1}^2}{Q_k(\sqrt{d} + P_{k+1})} = \frac{Q_k Q_{k+1}}{Q_k(\sqrt{d} + P_{k+1})} = \frac{1}{\alpha_{k+1}}.$$

■

Teorema 2.10 *Sea α un irracional cuadrático. Entonces su fracción continua simple es periódica.*

Demostración: Del teorema anterior, se tiene

$$\alpha = \frac{P_o + \sqrt{d}}{Q_0}$$

con $Q_0 | (P_0^2 - d)$. Consideremos

$$\alpha_k = \frac{P_k + \sqrt{d}}{Q_k}$$

$$a_k = [\![\ \alpha_k\ ]\!]$$

$$P_{k+1} = a_k Q_k - P_k$$

$$Q_{k+1} = \frac{d - P_{k+1}^2}{Q_k}$$

tenemos

$$P_0 = 0, \qquad P_1 = d,$$

$$Q_0 = 1, \qquad Q_1 = 1,$$

$$\alpha_0 = \sqrt{d^2 + 1}, \qquad \alpha_1 = d + \sqrt{d^2 + 1},$$

$$a_0 = d, \qquad a_1 = 2d$$

y $\alpha = [a_0, a_1, \ldots]$. Ahora,

$$\alpha = \frac{\alpha_k p_{k-1} + p_{k-2}}{\alpha_k q_{k-1} + q_{k-2}}$$

y si $\overline{\alpha}$ denota el $\mathbb{Q}$-conjugado de α (es decir, es la otra raíz del polinomio mínimo de α),

$$\overline{\alpha} = \frac{\overline{\alpha_k} p_{k-1} + p_{k-2}}{\overline{\alpha_k} q_{k-1} + q_{k-2}}, \text{ luego } \overline{\alpha_k} = -\frac{q_{k-2}}{q_{k-1}} \left(\frac{\overline{\alpha} - C_{k-2}}{\overline{\alpha} - C_{k-1}} \right).$$

Ahora $C_{k-1}, C_{k-2} \to \alpha$ cuando $k \to \infty$, entonces

$$\frac{\overline{\alpha} - C_{k-2}}{\overline{\alpha} - C_{k-1}} \to 1, k \to \infty.$$

Por lo tanto, $\overline{\alpha}_k < 0$, análogamente se verifica que $\alpha_k > 0$, $\alpha_k - \overline{\alpha}_k = \dfrac{2\sqrt{d}}{Q_k} > 0$, para todo k suficientemente grande. Tenemos que $Q_k Q_{k+1} = d - P_{k+1}^2 \leq d$ así

$$Q_k \leq Q_k Q_{k+1} = d - P_{k+1}^2 \leq d$$

y

$$P_{k+1}^2 \leq d - Q_k \leq d$$

para k suficientemente grande. Entonces existe únicamente un número finito de valores posibles para P_k, Q_k, concluimos así que existen enteros $i < j$ tales que $P_i = P_j, Q_i = Q_j$. Entonces $a_i = a_j$ y, así a_i se define recursivamente, tenemos finalmente que

$$\alpha = [a_0, a_1, \ldots, a_{i-1}, \ \overline{a_i, \ldots, a_{j-1}}\ ].$$

■

2.3. Transformaciones modulares

A continuación investigaremos cuándo dos irracionales tienen fracciones continuas *finalmente iguales*. Veremos que esto sucede cuando son equivalentes en el sentido siguiente.

Definición 2.4 *Dos números α y β son equivalentes si existen enteros racionales a, b, c, d tales que*

$$\alpha = \frac{a\beta + b}{c\beta + d}, \qquad ad - bc = \pm 1 \tag{2.3.1}$$

Se puede demostrar que dos números racionales cualesquiera son equivalentes entre sí, y que un número racional nunca es equivalente a uno irracional, por lo que nos limitaremos a considerar números irracionales. También puede verse que la fórmula anterior define una biyección sobre los números irracionales. Las biyecciones de este tipo se llaman *transformaciones modulares*. Las inversas y la composición de transformaciones modulares son de nuevo transformaciones modulares, por lo que la equivalencia de números irracionales (y en general de números reales) es una relación de equivalencia.

Consideremos la expresión para $\alpha = [a_0, \ldots, a_n, \beta]$ dada por

$$\alpha = \frac{p_n\beta + p_{n-1}}{q_n\beta + q_{n-1}}.$$

Los teoremas 2.2 y 2.7 garantizan que tal expresión define una transformación modular.

El siguiente teorema caracteriza las transformaciones modulares que se pueden expresar de esta forma.

Teorema 2.11 *Si una transformación modular (2.3.1) cumple que $c > d > 0$, entonces se puede expresar de la forma $\alpha = [a_0, a_1, a_2, \ldots, a_n, \beta]$ para ciertos enteros racionales $a_0, a_1, \ldots, a_n$ todos positivos salvo quizá el primero.*

Demostración: Probaremos que existen $a_0, a_1, \ldots, a_n$ tales que

$$p_n = a,\ p_{n-1} = b,\ q_n = c,\ q_{n-1} = d \tag{2.3.2}$$

lo probaremos por inducción sobre d. Si $d = 1$, tenemos que $a = bc \pm 1$. En el caso $a = bc + 1$ sirve $\alpha = [b, c, \beta]$ y si se cumple que $a = bc - 1$, entonces funciona $\alpha = [b - 1, 1, c - 1, \beta]$.

Supongamos ahora que $d > 1$. Aplicando el Teorema 2.1, las ecuaciones (2.3.1) equivalen a

$$p_{n-1} = b,\ p_{n-2} = a - a_n b,\ q_{n-1} = d,\ q_{n-2} = c - a_n d \tag{2.3.3}$$

así $b(c-a_nd)-(a-a_nb)d = \pm 1$ para cualquier a_n y por hipótesis de inducción (2.3.3) tendrá solución si garantizamos que $d > c - a_nd > 0$, o equivalentemente si $\frac{c}{d} > a_n > \frac{c-d}{d}$. Como $\frac{c}{d} - \frac{c-d}{d} = d > 1$, podemos tomar un número natural a_n en estas condiciones y así se cumple el teorema.

■

Teorema 2.12 *Dos números irracionales α y β son equivalentes si y sólo si sus desarrollos en fracción continua son finalmente iguales, es decir, si*

$$\alpha = [a_0, a_1, \ldots, a_m, c_0, c_1, \ldots], \qquad \beta = [b_0, b_1, \ldots, b_n, c_0, c_1, \ldots]$$

Demostración: Supongamos que α y β son finalmente iguales. Así el Teorema 2.7 nos da que en estas condiciones tanto α como β son equivalentes al número $[c_0, c_1, \ldots]$, luego son equivalentes entre sí (pues la relación es de equivalencia).

Ahora supóngase que α y β son equivalentes, es decir

$$\alpha = \frac{a\beta + b}{c\beta + d},\ \ ad - bc = \pm 1$$

podemos suponer sin pérdida de generalidad que $c\beta + d > 0$. Desarrollando $\beta = [b_0, b_1, \ldots, b_k, b_{k+1}, \ldots]$, tenemos

$$\beta = \frac{\beta'_k p_{k-1} + p_{k-2}}{\beta'_k q_{k-1} + q_{k-2}},\ \text{donde}\ \ \beta'_k = [b_{k+1}, b_{k+2}, \ldots],$$

realizando la composición de las transformaciones modulares obtenemos

$$\alpha = \frac{P\beta'_k + R}{Q\beta'_k + S}$$

donde

$$P = ap_{k-1} + bq_{k-1}$$

$$R = ap_{k-2} + bq_{k-2}$$

$$Q = cp_{k-1} + dq_{k-1}$$

$$S = cp_{k-2} + dq_{k-2}$$

que son enteros racionales y cumplen $PS - QR = \pm 1$, lo cual no es difícil de verificar.

Del Teorema 2.2 y puesto que β se encuentra entre dos convergentes consecutivos cualesquiera,

$$\left|\frac{p_{k-1}}{q_{k-1}} - \beta\right| < \frac{1}{q_{k-1}q_k}, \text{ luego } |p_{k-1} - \beta q_{k-1}| < \frac{1}{q_k}.$$

Por lo tanto

$$p_{k-1} = \beta q_{k-1} + \frac{\delta}{q_{k-1}}$$

$$p_{k-2} = \beta q_{k-2} + \frac{\delta'}{q_{k-2}}$$

con $|\delta|, |\delta'| < 1$.

De aquí

$$Q = (c\beta + d)q_{k-1} + \frac{c\delta}{q_{k-1}} \text{ y } S = (c\beta + d)q_{k-2} + \frac{c\delta'}{q_{k-2}}.$$

Teniendo en cuenta que $c\beta + d > 0$ y puesto que $\{q_k\}_{k\geq 1}$ es creciente, se sigue que $Q > S > 0$ para k suficientemente grande. Así aplicando el teorema anterior resulta que $\alpha = [a_0, a_1, \ldots, a_m, \beta'_k]$, por lo tanto α y β son finalmente iguales.

■

Capítulo 3

Aplicaciones de las fracciones continuas

En el capítulo anterior desarrollamos parte de la teoría básica de las fracciones continuas, en el presente ilustraremos algunas de sus aplicaciones.

3.1. Ecuación diofantina de primer grado.

A continuación describiremos una de las aplicaciones más comunes que nos permiten obtener las soluciones a ecuaciones diofantinas de primer grado.

Consideremos la ecuación diofantina

$$ax + by = c \tag{3.1.1}$$

donde $a, b, c \in \mathbb{Z}$ dados, x e y son incógnitas, la cual admite una infinidad de soluciones en $\mathbb{R}$, sin embargo si restringimos la condición de que $x, y \in \mathbb{Z}$ el número de soluciones puede ser limitado.

Estamos interesados en hallar la solución general de (3.1.1) en $\mathbb{Z}$, comenzaremos por considerar el caso particular más simple, a saber:

$$ax - by = \pm 1$$

donde sin pérdida de generalidad suponemos que $a, b \in \mathbb{Z}^+$ son primos relativos, es decir $(a, b) = 1$. Con las hipotésis anteriormente consideradas, resolveremos inicialmente la siguiente ecuación diofantina

$$ax - by = 1. \tag{3.1.2}$$

La ecuación $-ax + by = 1$ con $(a, b) = 1$ es de la misma forma que (3.1.2) salvo el cambio de posición de las variables x y y. Consideremos el siguiente resultado

Teorema 3.1 *La ecuación $ax - by = 1$, donde a y b son enteros positivos y $(a, b) = 1$, tiene infinidad de soluciones enteras (x, y).*

Demostración: Comencemos por obtener el desarrollo en fracción continua de $\frac{a}{b}$, la cual es finita, luego

$$\frac{a}{b} = [a_0, a_1, a_2, \ldots, a_{n+1}] \tag{3.1.3}$$

se tienen así las razones $C_0, C_1, C_2, \ldots, C_n, C_{n+1}$, consideremos las dos últimas

$$C_n = \frac{p_n}{q_n} \text{ y } C_{n+1} = \frac{p_{n+1}}{q_{n+1}} = \frac{a}{b},$$

éstas satisfacen las condiciones que establece la parte (i) del Teorema 2.2, es decir

$$p_n q_{n+1} - p_{n+1} q_n = (-1)^{n+1}$$

donde $p_{n+1} = a$ y $q_{n+1} = b$, lo cual implica que

$$aq_n - bp_n = (-1)^{n+2} = (-1)^n \tag{3.1.4}$$

si n es par, el número de coeficientes $a_0, a_1, a_2, \ldots, a_n, a_{n+1}$ es par y (3.1.4), se reescribe como:

$$aq_n - bp_n = 1 \tag{3.1.5}$$

que al compararla con la ecuación original $ax - by = 1$, obtenemos que una solución de esta última es $x_0 = q_n$ e $y_0 = p_n$. Esta solución es particular y no es la solución general, denotaremos la solución particular por (x_0, y_0).

Si n es impar, el número de coeficientes es impar y (3.1.4) se escribe como $ax - by = -1$, reescribiendo a (3.1.3)

$$\frac{a}{b} = [a_0, a_1, a_2, \ldots, a_{n+1} - 1, 1]$$

que posee así un número par de coeficientes, los cuales reenumeramos y luego calculamos $\frac{p_n}{q_n}$ y $\frac{p_{n+1}}{q_{n+1}} = \frac{a}{b}$, y la ecuación (3.1.5) nuevamente se satisface.

Obtenida una solución particular, a saber (x_0, y_0) de la ecuación, resulta sencillo obtener la solución general. Supongamos que (x, y) es otra solución de (3.1.2), es decir se satisface que

$$ax - by = 1 \quad \text{y} \quad ax_0 - by_0 = 1$$

de estas dos últimas ecuaciones aplicando sustracción, obtenemos

$$a(x - x_0) = b(y - y_0) \tag{3.1.6}$$

esto prueba que b divide al primer miembro de la igualdad, pero como $(a, b) = 1$, obtenemos que b divide a $x - x_0$, es decir existe $t \in \mathbb{Z}$ tal que

$$x - x_0 = tb, \quad \text{luego} \quad x = x_0 + tb$$

sustituyendo este valor en (3.1.6), obtenemos

$$a(tb) = b(y - y_0), \quad \text{por lo tanto} \quad y = y_0 + at$$

finalmente se tiene que cualquier solución (x, y) de la ecuación $ax - by = 1$, es de la forma

$$x = x_0 + bt, \qquad y = y_0 + at, \qquad t \in \mathbb{Z}. \tag{3.1.7}$$

Recíprocamente, si (x_0, y_0) es una solución particular de $ax - by = 1$, y si en (3.1.7) sustituimos cualquier entero t, ahora el valor de (x, y) satisface la ecuación dada, en efecto:

$$ax - by = a(x_0 + bt) - b(y_0 + at) = (ax_0 - by_0) + (tab - tab) = 1$$

Por lo tanto concluimos que los valores de x e y dados por (3.1.7) constituyen la solución general de la ecuación (3.1.2).

■

Ejemplo 1
Resolver la ecuación $205x - 93y = 1$.
Solución: Se verifica sin dificultad que 205 y 93 son primos relativos, obtengamos el desarrollo en fracción continua de

$$\frac{205}{93} = [2, 4, 1, 8, 2]$$

la cual consta de un número impar de coeficientes, sin embargo podemos reescribirla en la siguiente forma

$$\frac{205}{93} = [2, 4, 1, 8, 1, 1]$$

la cual posee un número par de coeficientes, calculando C_k, obtenemos

$$C_0 = \frac{2}{1} \qquad C_2 = \frac{11}{5} \qquad C_4 = \frac{108}{49}$$

$$C_1 = \frac{9}{4} \qquad C_3 = \frac{97}{44} \qquad C_5 = \frac{205}{93} = \frac{a}{b}$$

de (3.1.7), se tiene que la solución general a nuestra ecuación es:

$$x = 49 + 93t, \qquad y = 108 + 205t, \qquad t \in \mathbb{Z}.$$

■

Con la condición de que a y b son primos relativos, resolveremos ahora la ecuación

$$ax - by = -1. \tag{3.1.8}$$

El método para resolver (3.1.8) es análogo al usado para resolver (3.1.2). Basta transformar $\frac{a}{b}$ en una fracción continua con un número impar de coeficientes, en tal caso la ecuación (3.1.4) deriva en

$$aq_n - bp_n = (-1)^n = -1,$$

comparando esta ecuación con $ax - by = -1$, obtenemos que $x_0 = q_n$ e $y_0 = p_n$, siendo ésta una solución particular de (3.1.8), mientras que la solución general es como antes

$$x = x_0 + bt, \qquad y = y_0 + at, \qquad t \in \mathbb{Z}. \tag{3.1.9}$$

Ejemplo 2
Resolver la ecuación $205x - 93y = -1$.
Solución: del ejemplo 1, obtenemos

$$\frac{205}{93} = [2, 4, 1, 8, 2]$$

la cual consta de un número impar de coeficientes, se obtiene así que la solución general de nuestra ecuación es

$$x = 44 + 93t, \qquad y = 97 + 205t, \qquad t \in \mathbb{Z}.$$

■

Con la hipótesis de que a y b son primos relativos, discutiremos el procedimiento para obtener la solución general de la ecuación

$$ax - by = c. \tag{3.1.10}$$

Conocemos las soluciones de la ecuación (3.1.2), entonces resulta fácil hallar las soluciones a la ecuación (3.1.10), sea como antes (x_0, y_0) una solución particular de (3.1.2), es decir

$$ax_0 - by_0 = 1$$

multiplicando esta expresión por c, obtenemos

$$a(cx_0) - b(cy_0) = c$$

entonces (cx_0, cy_0) es una solución particular de la ecuación (3.1.10), por lo tanto su solución general es

$$x = cx_0 + bt, \qquad y = cy_0 + at, \qquad t \in \mathbb{Z}. \tag{3.1.11}$$

Ejemplo 3
Hallar las soluciones enteras de la ecuación $205x - 93y = -5$.
Solución: Del ejemplo 1, obtenemos que una solución particular a la ecuación $205x - 93y = 1$ es $x_0 = 49$ e $y_0 = 108$, de acuerdo con (3.1.11) la solución general queda descrita por

$$x = -245 + 93t, \qquad y = -540 + 205t, \qquad t \in \mathbb{Z}.$$

por ejemplo si $t = 2$ la solución es $(x, y) = (-59, -130)$, en efecto pues

$$205(-59) - 93(-130) = -12095 + 12090 = -5.$$

■

Analicemos ahora la solución general de la ecuación

$$ax + by = c \tag{3.1.12}$$

con $a, b \in \mathbb{Z}^+, (a, b) = 1$, el procedimiento para resolver esta ecuación es similar (salvo una pequeña modificación) al método discutido para la ecuación $ax - by = c$. Como antes expresemos a $\frac{a}{b}$ como una fracción continua con un número par de coeficientes, de donde obtenemos p_n y q_n, como antes $aq_n - bp_n = 1$.

El artificio consiste en escribir la ecuación (3.1.12) en la forma

$$ax + by = c \cdot 1 = c(aq_n - bp_n)$$

simplificando obtenemos

$$a(cq_n - x) = b(y + cp_n) \tag{3.1.13}$$

por la hipótesis se sigue que $b|(cq_n - x)$, lo que implica que existe $t \in \mathbb{Z}$ tal que $bt = cq_n - x$, así

$$x = cq_n - bt \tag{3.1.14}$$

sustituyendo (3.1.14) en (3.1.13) y simplificando, obtenemos

$$y = at - cp_n. \tag{3.1.15}$$

Recíprocamente, sea t cualquier entero, sustituyendo (3.1.14) y (3.1.15) en $ax + by = c$, obtenemos

$$ax+by = a(cq_n-tb)+b(at-cp_n) = acq_n-tab+tab-bcp_n = c(aq_n-bp_n) = c$$

y la ecuación (3.1.12) se satisface, por lo tanto la solución general de la ecuación $ax + by = c$, es

$$x = cq_n - bt, \qquad y = at - cp_n, \qquad t \in \mathbb{Z}. \tag{3.1.16}$$

Ejemplo 4
Hallar las soluciones enteras de la ecuación $13x + 17y = 300$.
Solución: Aplicando el método utilizado en el ejemplo 1, se obtiene que una solución particular a la ecuación $13x-17y = 1$ es $(4, 3)$, así $13(4)-17(3) = 1$, así la ecuación a resolver puede reescribirse como

$$13x + 17y = 300(13(4) - 17(3))$$

obtenemos finalmente que la solución general, aplicando (3.1.14) y (3.1.15), es

$$x = 1200 - 17t, \qquad y = 13t - 900, \qquad t \in \mathbb{Z}.$$

■

Finalmente hallemos la solución a la ecuación general

$$Ax \pm By = \pm C \tag{3.1.17}$$

Multiplicando eventualmente por -1 obtenemos alguna ecuación de la forma

$$\pm Ax \pm By = C$$

ésta se reduce a una de las dos formas siguientes

$$Ax + By = \pm C \qquad\qquad Ax - By = \pm C \tag{3.1.18}$$

donde $A, B \in \mathbb{Z}^+$. Por ejemplo, de las 4 ecuaciones

$$3x + 7y = 10, \qquad 3x - 7y = 10 \qquad -3x - 7y = 10, \qquad -3x + 7y = 10$$

las dos primeras son ya de la forma (3.1.18), y las otras dos pueden sustituirse respectivamente por

$$3x + 7y = -10, \qquad\qquad 3x - 7y = -10.$$

No todas las ecuaciones de la forma (3.1.18) admiten solución entera, en efecto:

Sea $d = (A, B)$. Si d no divide a C, ninguna de las ecuaciones (3.1.18) admiten solución entera, porque el primer miembro de la igualdad es divisible por d mientras que el segundo no lo es. Por otra parte, si d divide a C, podemos dividir toda la ecuación por d, reduciendola así a una de las formas ya tratadas, es decir:

$$ax + by = c \qquad \text{o} \qquad ax - by = c \tag{3.1.19}$$

donde $(a, b) = 1$, y éstas ya sabemos resolverlas. Recíprocamente, alguna solución de alguna de las ecuaciones (3.1.19) será automáticamente solución de (3.1.18).

Ejemplo 5
Resolver la ecuación $410x - 186y = 10$.
Solución: Tenemos que $(410, 186) = 2$, donde $2|10$, así la ecuación admite solución entera. Dividiendo la ecuación por 2, obtenemos:

$$205x - 93y = 5$$

como $(205, 93) = 1$, aplicando el método del ejemplo 3, llegamos a que la solución general de $410x - 186y = 10$ es:

$$x = 245 + 93t, \qquad y = 540 + 205t, \qquad t \in \mathbb{Z}.$$

■

3.2. La fracción continua de e

Recordemos que en el Capítulo 2, se concluyó que cualquier número real admite un desarrollo en la forma de fracción continua, en esta sección estaremos interesados en estudiar la fracción continua del número e, la cual resulta ser la siguiente:

$$e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \ldots]$$

Recordemos que la función exponencial e^x es continua en $\mathbb{R}$, más aún es infinitamente diferenciable en $\mathbb{R}$, así admite un desarrollo en serie de Taylor, a saber

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

Para lograr nuestro objetivo requeriremos desarrollar algunos resultados.

Fijemos un número natural m ($m \in \mathbb{N}$) y para cada $n \geq 0$, definamos

$$\psi_n = \sum_{r=0}^{\infty} \frac{2r + 2n + 1}{1 \cdot 3 \cdot 5 \ldots (2r + 2n + 1)} \cdot \frac{2r + 2}{2 \cdot 4 \cdot 6 \ldots (2r + 2)} \cdot \frac{1}{m^{2r}}$$

Si $m > 1$, se concluye fácilmente que se cumple la siguiente desigualdad

$$\psi_n \leq \sum_{r=0}^{\infty} \left(\frac{1}{m}\right)^r = \frac{m}{m-1}$$

es decir, ψ_n está acotada superiormente para toda $m > 1$.

Por otra parte haciendo uso del desarrollo en serie de Taylor de la exponencial, realizamos el siguiente cálculo

$$e^{1/m} + e^{-1/m} = \sum_{k=0}^{\infty} \frac{1}{k!m^k} + \sum_{k=0}^{\infty} \frac{(-1)^k}{k!m^k} = \sum_{k=0}^{\infty} \frac{1}{k!m^k}(1 + (-1)^k)$$

$$= \sum_{n=0}^{\infty} \frac{1 + (-1)^{2n}}{(2n)!m^{2n}} + \sum_{n=0}^{\infty} \frac{1 + (-1)^{2n+1}}{(2n+1)!m^{2n+1}}$$

$$= \sum_{n=0}^{\infty} \frac{2}{(2n)!m^{2n}} = 2\sum_{r=0}^{\infty} \frac{1}{(2r)!m^{2r}}$$

$$= 2\sum_{r=0}^{\infty} \frac{(2r+1)(2r+2)}{(2r)!(2r+1)(2r+2)} \frac{1}{m^{2r}} = 2\psi_0$$

por lo tanto

$$\psi_0 = \frac{1}{2}(e^{1/m} + e^{-1/m}).$$

Análogamente puede verificarse sin dificultad que

$$e^{1/m} - e^{-1/m} = \frac{2}{m} \sum_{r=0}^{\infty} \frac{1}{(2r+1)!m^{2r}} = \frac{2}{m}\psi_1$$

de donde obtenemos

$$\psi_1 = \frac{m}{2}(e^{1/m} - e^{-1/m}).$$

El siguiente resultado establece una relación muy importante que se da en la sucesión $\{\psi_n\}_{n\geq 0}$.

Teorema 3.2 *Sea m número natural no nulo fijo y ψ_n definido como antes. Entonces se satisface*

$$m^2\psi_n = (2n+1)m^2\psi_{n+1} + \psi_{n+2}, \qquad n \in \mathbb{N}_0. \tag{3.2.1}$$

Demostración: En efecto, desarrollemos la expresión

$$m^2\psi_n - (2n+1)m^2\psi_{n+1} = m^2 \sum_{r=0}^{\infty} \frac{2r+2n+1}{1\cdot 3\cdots(2r+2n+1)} \frac{2r+2}{2\cdot 4\cdots(2r+2)} \frac{1}{m^{2r}}$$

$$- (2n+1)m^2 \sum_{r=0}^{\infty} \frac{2r+2(n+1)+1}{1\cdot 3\cdots[2r+2(n+1)+1]} \frac{2r+2}{2\cdot 4\cdots(2r+2)} \frac{1}{m^{2r}}$$

$$= \sum_{r=0}^{\infty} \frac{(2r+2n+1)(2r+2n+3)(2r+2)}{1\cdot 3\cdots(2r+2n+1)(2r+2n+3)\cdot 2\cdot 4\cdots(2r+2)} \frac{1}{m^{2(r-1)}}$$

$$- \sum_{r=0}^{\infty} \frac{(2n+1)(2r+2n+3)(2r+2)}{1\cdot 3\cdots(2r+2n+3)\cdot 2\cdot 4\cdots(2r+2)} \frac{1}{m^{2(r-1)}}$$

$$= \sum_{r=0}^{\infty} \frac{[(2r+2n+1)-(2n+1)](2r+2n+3)}{1\cdot 3\cdot 5\cdots(2r+2n+3)} \frac{2r+2}{2\cdot 4\cdots(2r+2)} \frac{1}{m^{2(r-1)}}$$

$$= \sum_{r=0}^{\infty} \frac{2r(2r+2n+3)}{1\cdot 3\cdots(2r+2n+3)} \frac{2r+2}{2\cdot 4\cdots(2r+2)} \frac{1}{m^{2(r-1)}}$$

$$= \sum_{r=1}^{\infty} \frac{2r(2r+2n+3)}{1\cdot 3\cdot 5\cdots(2r+2n+3)} \frac{2r+2}{2\cdot 4\cdots(2r+2)} \frac{1}{m^{2(r-1)}}$$

$$= \sum_{r=0}^{\infty} \frac{2(r+1)[2(r+1)+2n+3]}{1\cdot 3\cdots[2(r+1)+2n+3]} \frac{2(r+1)+2}{2\cdot 4\cdots[2(r+1)+2]} \frac{1}{m^{2r}}$$

$$= \sum_{r=0}^{\infty} \frac{2r+2n+5}{1\cdot 3\cdots(2r+2n+5)} \frac{2(r+1)(2r+4)}{2\cdot 4\cdots(2r+4)} \frac{1}{m^{2r}}$$

$$= \sum_{r=0}^{\infty} \frac{2r+2(n+2)+1}{1\cdot 3\cdot 5\cdots[2r+2(n+2)+1]} \frac{2r+2}{2\cdot 4\cdots(2r+2)} \frac{1}{m^{2r}}$$

$$= \psi_{n+2}$$

■

Por el teorema anterior concluimos que las series son convergentes, además $\psi_n > 0, \forall\, n \in \mathbb{N}_0$, por lo tanto podemos definir

$$w_n = \frac{m\psi_n}{\psi_{n+1}}, \qquad n \in \mathbb{N}_0.$$

Dividiendo por $m\psi_{n+1}$ a la ecuación descrita en (3.2.1) obtenemos la expresión siguiente

$$w_n = (2n+1)m + \frac{1}{w_{n+1}}, \qquad n = 0, 1, 2, \ldots$$

de donde se sigue que $w_n > 1$ para todo n, y que el desarrollo en fracción continua de w_0 es

$$w_0 = m + \frac{1}{w_1} = m + \cfrac{1}{3m + \cfrac{1}{w_2}} = m + \cfrac{1}{3m + \cfrac{1}{5m + \cfrac{1}{w_3 + \cdots}}}$$

obtenemos así

$$w_0 = [m, 3m, 5m, \ldots].$$

Además,

$$w_0 = \frac{m\psi_0}{\psi_1} = \frac{e^{1/m} + e^{-1/m}}{e^{1/m} - e^{-1/m}} = \frac{e^{2/m} + 1}{e^{2/m} - 1},$$

con lo cual haciendo $m = 2$ obtenemos en particular el siguiente desarrollo en fracción continua

$$\frac{e+1}{e-1} = [2, 6, 10, 14, \ldots],$$

se observa que esta fracción continua es infinita lo cual indica que representa a un número irracional, lo que prueba que el número e no es racional, más aún, que no es un irracional cuadrático, pues la fracción continua es no periódica.

Consideremos ahora la expresión general para m, es decir

$$w_0 = \frac{e^{2/m} + 1}{e^{2/m} - 1}, \text{ por lo que } w_0(e^{2/m} - 1) = e^{2/m} + 1,$$

de donde obtenemos

$$e^{2/m} = \frac{w_0 + 1}{w_0 - 1} = 1 + \frac{2}{w_0 - 1}, \text{ luego } e^{2/m} + 1 = 2 + \frac{2}{w_0 - 1}$$

lo cual implica que

$$\frac{e^{2/m} + 1}{2} = 1 + \frac{1}{w_0 - 1}$$

Utilicemos ahora la siguiente notación

$$\xi = \frac{e^{2/m} + 1}{2} = 1 + \frac{1}{w_0 - 1}.$$

Se obtiene claramente que $\xi = [1, m-1, 3m, 5m, \ldots]$. Para obtener el desarrollo de la fracción continua de e, necesitamos eliminar el 2 del denominador de

ξ. Denotemos por $\eta = e^{2/m} = 2\xi - 1$. Expondremos un método que nos permite calcular en muchos casos la fracción continua de un número η a partir de la fracción continua de un número ξ cuando entre ellos se da una relación del tipo

$$\eta = \frac{u\xi + v}{w},$$

donde u y w son números naturales y v es un número entero.

Antes de enunciar el resultado principal recordemos que un número racional siempre admite un desarrollo en fracción continua de longitud par y otro de longitud impar, es decir que si $a > 1$, entonces

$$[\ldots, a] = [\ldots, a-1, 1].$$

También es importante notar que las fórmulas del Teorema 2.1 son válidas para $n = 0, 1$, si convenimos en que $p_{-1} = 1, q_{-1} = 0, p_{-2} = 0, q_{-2} = 1$.

Teorema 3.3 *Considere* $[a_0, a_1, a_2, \ldots]$ *el desarrollo en fracción continua de el irracional* ξ. *Sea* $\frac{p_n}{q_n}$ *el convergente* n*-ésimo y* $\xi_n = [a_n, a_{n+1}, a_{n+2}, \ldots]$. *Sea* $\eta = \frac{u\xi + v}{w}$, *donde* u, v, w *son números enteros,* $u > 0, w > 0, uw = D > 1$. *Para un índice cualquiera* $n \geq 1$ *desarrollamos el número racional*

$$\frac{u[a_0, a_1, a_2, \ldots, a_{n-1}] + v}{w} = \frac{up_{n-1} + vq_{n-1}}{wq_{n-1}} = [b_0, b_1, b_2, \ldots, b_{m-1}]$$

eligiendo el final de modo que $m \equiv n \mod 2$. *Sea* $\frac{r_j}{s_j}$ *el* j*-ésimo convergente de este desarrollo, de modo que en particular se tiene*

$$\frac{up_{n-1} + vq_{n-1}}{wq_{n-1}} = \frac{r_{m-1}}{s_{m-1}}. \tag{3.2.2}$$

Entonces existen números enteros u', v', w' *tales que*

$$\begin{pmatrix} u & v \\ 0 & w \end{pmatrix} \begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix} = \begin{pmatrix} r_{m-1} & r_{m-2} \\ s_{m-1} & s_{m-2} \end{pmatrix} \begin{pmatrix} u' & v' \\ 0 & w' \end{pmatrix}$$

$u' > 0,\ w' > 0,\ u'w' = D,\ -w' \leq v' \leq u',\ y\ \eta = [b_0, b_1, \ldots, b_{m-1}, \eta_m],\ donde\ \eta_m = \dfrac{u'\xi_n + v'}{w'}$.

Demostración: De la ecuación matricial obtenemos el siguiente sistema de ecuaciones:

$$up_{n-1} + vq_{n-1} = r_{m-1}u' \tag{3.2.3}$$

$$wq_{n-1} = s_{m-1}u' \tag{3.2.4}$$

$$up_{n-2} + vq_{n-2} = r_{m-1}v' + r_{m-2}w' \tag{3.2.5}$$

$$wq_{n-2} = s_{m-1}v' + s_{m-2}w' \tag{3.2.6}$$

Como r_{m-1} y s_{m-1} son primos relativos, de (3.2.2) se sigue que los cocientes

$$\frac{up_{n-1} + vq_{n-1}}{r_{m-1}} = \frac{wq_{n-1}}{s_{m-1}}$$

son un mismo número entero u' que satisface (3.2.3) y (3.2.4). Considerando el segundo cociente concluimos que $u' > 0$.

Las ecuaciones (3.2.5) y (3.2.6) forman un sistema de ecuaciones lineales con determinante ± 1, luego tiene solución entera (v', w'). Ahora tomando determinante en la ecuación matricial, obtenemos que

$$uw(-1)^{n-2} = (-1)^{m-2}u'w',\ \text{luego}\ \ uw = (-1)^{m-n}u'w',$$

y puesto que $m \equiv n \mod 2$, tenemos que $m - n = 2k$ para algún $k \in \mathbb{Z}$, concluimos que $D = uw = u'w'$, de donde deducimos además que $w' > 0$. De (3.2.6) obtenemos

$$v' = \frac{wq_{n-2} - s_{m-2}w'}{s_{m-1}} \geq -\frac{s_{m-2}}{s_{m-1}}w' \geq -w',$$

ahora usando nuevamente (3.2.6) y además (3.2.4) obtenemos que

$$v' = \frac{wq_{n-2} - s_{m-2}w'}{s_{m-1}} \leq \frac{w}{s_{m-1}}q_{n-2} = \frac{q_{n-2}}{q_{n-1}}u' \leq u'.$$

por lo tanto $-w' \leq v' \leq u'$. Ahora por las hipótesis y el Teorema 2.7, se tiene

$$\xi = \frac{p_{n-1}\xi_n + p_{n-2}}{q_{n-1}\xi_n + q_{n-2}}.$$

Haciendo uso de esto y las ecuaciones que definen a $u',\ v',\ w'$, se obtiene lo siguiente

$$\eta = \frac{u\xi + v}{w} = \frac{u(p_{n-1}\xi_n + p_{n-2}) + v(q_{n-1}\xi_n + q_{n-2})}{w(q_{n-1}\xi_n + q_{n-2})}$$

$$= \frac{(up_{n-1} + vq_{n-1})\xi_n + (up_{n-2} + vq_{n-2})}{wq_{n-1}\xi_n + wq_{n-2}}$$

$$= \frac{r_{m-1}u'\xi_n + r_{m-1}v' + r_{m-2}w'}{s_{m-1}u'\xi_n + s_{m-1}v' + s_{m-2}w'}$$

$$= \frac{r_{m-1}\dfrac{u'\xi_n + v'}{w'} + r_{m-2}}{s_{m-1}\dfrac{u'\xi_n + v'}{w'} + s_{m-2}}$$

de donde, definiendo $\eta_m = \dfrac{u'\xi_n + v'}{w'}$, concluimos que

$$\eta = \frac{r_{m-1}\eta_m + r_{m-2}}{s_{m-1}\eta_m + s_{m-2}}$$

concluimos finalmente

$$\eta = [b_0, b_1, b_2, \ldots, b_{m-1}, \eta_m].$$

■

Del teorema anterior observamos que se cumple

$$\eta_m = \frac{u'\xi_n + v'}{w'} > \frac{v'}{w'} \geq -1$$

Más aún, si $a_n \geq D$, teniendo en cuenta que a_n es la parte entera de ξ_n, tenemos

$$\eta_m = \frac{u'\xi_n + v'}{w'} > \frac{u'D + v'}{w'} \geq \frac{u'^2 w' - w'}{w'} = u'^2 - 1 \geq 0,$$

y si $a_n \geq 2D$, entonces

$$\eta_m = \frac{u'\xi_n + v'}{w'} > \frac{u'2D + v'}{w'} \geq \frac{2u'^2 w' - w'}{w'} = 2u'^2 - 1 \geq 1.$$

Esto es importante porque cuando $\eta_m > 1$, la relación

$$\eta = [b_0, b_1, b_2, \ldots, b_{m-1}, \eta_m]$$

indica que los coeficientes de la fracción continua de η_m son la prolongación del desarrollo de η en fracción continua, que comienza con

$$[b_0, b_1, b_2, \ldots, b_{m-1}, \ldots].$$

Es fácil ver que esto sigue siendo cierto cuando $\eta_m \geq 0$ si convenimos en que

$$[\ldots, a, 0, b, c, \ldots] = [\ldots, a + b, c, \ldots].$$

Ahora nuestra intención es partir de un número irracional ξ_0 y dividir su fracción continua en secciones

$$\xi_0 = [a_0, \ldots, a_{n_1-1} | a_{n_1}, \ldots, a_{n_2-1} | a_{n_2}, \ldots, a_{n_3-1} | a_{n_3}, \ldots]$$

a las que aplicaremos sucesivamente el teorema anterior.

Dado $\eta_0 = \dfrac{u_0\xi_0 + v_0}{w_0}$ tal que $u_0,\ w_0 > 0$ y $D = u_0 w_0 > 1$, el teorema nos da números $u_1,\ v_1,\ w_1$ en las mismas condiciones (con el mismo D) y $b_0, b_1, \ldots, b_{m_1-1}$ tales que

$$\eta_0 = [b_0, b_1, \ldots, b_{m_1-1}, \eta_{m_1}] \quad \text{con} \quad \eta_{m_1} = \frac{u_1\xi_{n_1} + v_1}{w_1}.$$

Ahora aplicamos el teorema a $\xi_{n_1} = [a_{n_1}, \ldots, a_{n_2-1}|a_{n_2}, \ldots, a_{n_3-1}|a_{n_3}, \ldots]$ y obtenemos números $u_2,\ v_2,\ w_2$ con el mismo D y $b_{m_1}, \ldots, b_{m_2-1}$ tales que

$$\eta_{m_1} = [b_{m_1}, \ldots, b_{m_2-1}, \eta_{m_2}] \quad \text{con} \quad \eta_{m_2} = \frac{u_2\xi_{n_2} + v_2}{w_2}.$$

Suponiendo que $b_{m_1} \geq 0$ podemos enlazar ambos pasos y escribir

$$\eta_0 = [b_0, \ldots, b_{m_1-1}, \eta_{m_1}] = [b_0, \ldots, b_{m_1-1}|b_{m_1}, \ldots, b_{m_2-1}, \eta_{m_2}].$$

A continuación aplicamos el teorema a $\xi_{n_2} = [a_{n_2}, \ldots, a_{n_3-1}|a_{n_3}, \ldots]$, y así sucesivamente. De este modo vamos obteniendo el desarrolo en fracción continua de η_0, suponiendo que los sucesivos b_{m_i} que vamos obteniendo no sean negativos. Una forma de garantizarlo es partir la fracción original de modo que cada $a_{n_i} \geq D$, aunque no es necesario.

Con la ayuda del teorema siguiente podremos garantizar que, con las hipótesis adecuadas, al cabo de un número finito de pasos entramos en un ciclo que nos dará una fórmula general para el desarrollo completo de η_0. Al mismo tiempo nos dará una técnica útil para simplificar los cálculos.

Teorema 3.4 *Con las hipótesis del Teorema* 3.3*, si sustituimos a_0 por otro número congruente a él módulo D, digamos $a_0 + Dg$ (pero mantenemos los mismos $a_1, a_2, \ldots, a_{n-1}$) entonces se obtienen los mismos números u', v', w', así como los mismos m y $b_1, \ldots, b_{m-1}$. Además el número b_0 se transforma en $b_0 + u^2 g$.*

Demostración: Claramente

$$\begin{aligned}\frac{u[a_0+Dg,a_1,\ldots,a_{n-1}]+v}{w} &= \frac{u[a_0,a_1,\ldots,a_{n-1}]+v}{w}+\frac{uDg}{w}\\ &= \frac{u[a_0,a_1,\ldots,a_{n-1}]+v}{w}+\frac{uuwg}{w}\\ &= \frac{u[a_0,a_1,\ldots,a_{n-1}]+v}{w}+u^2g.\end{aligned}$$

Según el Teorema 3.3 el desarrollo de este número es

$$[b_0,b_1,\ldots,b_{m-1}]+u^2g=[b_0+u^2g,b_1,\ldots,b_{m-1}],$$

luego es claro que con el cambio todos los coeficientes quedaron igual salvo el primero que se incrementó en u^2g. Las relaciones recurrentes que determinan los denominadores de los convergentes no dependen del primer término de la fracción continua, luego los números q_i y s_i permanecen invariantes. La fórmula (3.2.4) nos da que u' tampoco varía. Por último, la ecuación (3.2.6) garantiza la conservación de v'.

■

Con esto tenemos en realidad un método general para calcular las fracciones continuas de números η_0 a partir de números ξ_0, pero explicaremos mejor este método aplicándolo al caso que nos interesa. Digamos sólo en general que si aplicamos sucesivamente el Teorema 3.3, las ternas (u_i,v_i,w_i) que vamos obteniendo varían en un conjunto finito (a causa de las restricciones que impone el teorema), luego después de un número finito de pasos volveremos a la misma terna.

Recordemos que si $\xi_0=\dfrac{e^{2/m}+1}{2}$, habíamos calculado

$$\xi_0=[1,m-1,3m,5m,\ldots] \tag{3.2.7}$$

y que $\eta_0=e^{2/m}=2\xi_0-1$. En este caso $u=2,\ v=-1,\ w=1$. Como $D=2$, para obtener congruencias módulo 2 haremos $m=2t$ (y después estudiaremos el caso $m=2t+1$). Dividimos la fracción de este modo:

$$\xi_0 = [1|2t-1|6t|10t|14t|\ldots].$$

Vamos a aplicar el Teorema 3.3 a cada segmento. El Teorema 3.4 nos dice que podemos sustituir cada coeficiente por otro congruente módulo 2 . Por ejemplo podemos considerar

$$\xi_0^* = [1|1|0|0|0|\ldots].$$

Ciertamente esto no tiene sentido como fracción continua, pero los cálculos a realizar sí lo tienen porque cada uno de ellos sólo involucra a un segmento, es decir a una fracción [1] ó [0] que sí es correcta. Al hacer los cálculos obtendremos para cada segmento unos coeficientes $|b_{m_i}, \ldots, b_{m_{i+1}-1}|$, que serán los que buscamos salvo el primero. A estos primeros coeficientes obtenidos tendremos que sumarles las cantidades $0,\ u_1^2(t-1),\ u_2^2 3t,\ u_3^2 5t, \ldots$ respectivamente.

Aplicamos el Teorema 3.3 al primer segmento:

$$\frac{u_0[1]+v_0}{w_0} = \frac{2[1]-1}{1} = 1 = [1] = [b_0],\ m=1$$

$$\begin{pmatrix} p_0 & p_{-1} \\ q_0 & q_{-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} r_0 & r_{-1} \\ s_0 & s_{-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} u_0 & v_0 \\ 0 & w_0 \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ 0 & 1 \end{pmatrix}.$$

Así, la ecuación matricial es

$$\begin{pmatrix} 2 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} u_1 & v_1 \\ 0 & w_1 \end{pmatrix}$$

y la solución:

$$\begin{pmatrix} u_1 & v_1 \\ 0 & w_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}.$$

Ahora aplicamos el teorema al segundo segmento [1]:

$$\frac{1[1]+0}{2} = \frac{1}{2} = [0,2] = [0,1,1] = [b_1, b_2, b_3],$$

donde hemos tomado el desarrollo con tres cifras para que la longitud sea impar, como la de [1] (para que sus longitudes sean congruentes módulo 2). Ahora

$$\begin{pmatrix} r_2 & r_1 \\ s_2 & s_1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 2 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} u_2 & v_2 \\ 0 & w_2 \end{pmatrix}$$

de donde obtenemos que

$$\begin{pmatrix} u_2 & v_2 \\ 0 & w_2 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 2 \end{pmatrix}$$

Sólo hay que rectificar el valor de b_1, que en realidad es $u_1^2(t-1) = t-1 \geq 0$, luego por ahora tenemos que $\eta_0 = [1|t-1,1,1|\ldots]$.

La siguiente aplicación del teorema es al segmento [0]:

$$\frac{1[0]-1}{2} = -\frac{1}{2} = [-1,1,1] = [b_4, b_5, b_6].$$

$$\begin{pmatrix} 1 & -1 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ 2 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ 2 & 0 \end{pmatrix}\begin{pmatrix} u_3 & v_3 \\ 0 & w_3 \end{pmatrix},$$

esta vez llegamos a que

$$\begin{pmatrix} u_3 & v_3 \\ 0 & w_3 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} u_2 & v_2 \\ 0 & w_2 \end{pmatrix},$$

el valor corregido de b_4 es $b_4 = -1 + u_2^2 3t = 3t - 1 \geq 0$.

Tenemos, pues, que $\eta_0 = [1|t-1,1,1|3t-1,1,1|\ldots]$.

Ahora bien, para los cálculos relativos al cuarto segmento partimos exactamente de los mismos datos que para el tercero (la fracción [0] y la terna $(u_3, v_3, w_3) = (1, -1, 2)$), luego llegaremos exactamente a los mismos coeficientes $[-1, 1, 1]$, y otra vez a la misma terna. Lo único que cambiará será la corrección del primer coeficiente, que ahora será $5t$, y después $7t$, etc., dando lugar siempre a coeficientes mayores que 0.

Consecuentemente tenemos la fracción continua de η_0, que es

$$\eta_0 = [1, t-1, 1, 1, 3t-1, 1, 1, 5t-1, 1, 1, 7t-1, 1, \ldots]$$

o más brevemente

$$e^{1/t} = \eta_0 = [\overline{1, (2k+1)t-1, 1}]_{k=0}^{\infty}.$$

En el caso $t = 1$ aparece un cero que debe ser cancelado y obtenemos:

$$e = [1, 0, 1, 1, 2, 1, 1, 4, 1, 1, 6, \ldots] = [2, 1, 2, 1, 1, 4, 1, 1, 6, \ldots],$$

así,

$$e = [2, \overline{1, 2k, 1}]_{k=1}^{\infty}.$$

En general, este método puede ser aplicado siempre que la fracción continua de ξ_0 pueda ser dividida en segmentos que (por lo menos desde uno dado en adelante) tengan todos la misma longitud y los mismos términos, salvo quizá el primero, y de modo que los primeros términos de cada segmento sean mayores o iguales que D (para que los coeficientes que obtengamos puedan ser enlazados) y congruentes módulo D (para que podamos reducirlos a constantes por el Teorema 3.4 y así llegar a un ciclo como ha ocurrido en el ejemplo).

Otra aplicación la tenemos cuando hacemos $m = 2t + 1$ en la expresión (3.2.7). Entonces queda

$$\xi_0 = [1|2t|6t+3|10t+5|14t+7|\ldots],$$

y con este método podemos calcular la fracción continua de $e^{2/(2t+1)}$. Para ello reducimos módulo 2 a la fracción $\xi_0^* = [1|0|1|1|1|\ldots]$.

Esta vez obtenemos las ternas

$$(2,-1,1),\ \ (1,0,2),\ \ (2,0,1),\ \ (1,0,2),\ \ (1,-1,2),\ \ (2,0,1).$$

La primera repetición $(u_1,v_1,w_1) = (u_3,v_3,w_3)$ no es significativa, pues los primeros (y únicos) coeficientes de los segmentos primero y tercero son [0] y [1] respectivamente, luego no son congruentes y por lo tanto no podemos garantizar que comience un ciclo (y de hecho no comienza).

En cambio la repetición $(u_5,v_5,w_5) = (u_2,v_2,w_2)$ sí cierra el proceso. La fracción que obtenemos es

$$\eta_0^* = [1|0|2|0,1,1|0|2|0,1,1|0|2|0,1,1|0|2|0,1,1|\ldots].$$

Para corregir los primeros coeficientes observamos que al pasar de ξ_0 a ξ_0^* hemos restado $2\cdot 0,\ 2t,\ 2(3t+1),\ 2(5t+2),\ 2(7t+3),\ldots$ así como que los valores de u_i son 2,1,2,1,1,2,1,1,2,1,1,2,... . Por lo tanto ahora hemos de sumar

$$0,\ t,\ 4(3t+1),\ 5t+2,\ 7t+3,\ 4(9t+5),\ 11t+7,\ 13t+9,\ 4(15t+11),\ \ldots$$

Omitimos los detalles, pero no es difícil llegar a que la expresión final es

$$e^{2/(2t+1)} = [1,\overline{(1+6k)t+3k,(12+24k)t+6+12k,(5+6k)t+2+3k,1,1}]_{k=0}^{\infty}$$

$$= [\overline{1,(1+6k)t+3k,(12+24k)t+6+12k,(5+6k)t+2+3k,1}]_{k=0}^{\infty}$$

La fórmula se simplifica bastante en el caso $t=0$, que nos da

$$e^2 = [\overline{1,3k,6+12k,2+3k,1}]_{k=0}^{\infty}$$

$$= [1,0,6,\overline{2+3k,1,1,3+3k,18+12k}]_{k=0}^{\infty}$$

$$= [7,\overline{2+3k,1,1,3+3k,18+12k}]_{k=0}^{\infty}$$

Explícitamente:

$$e^2 = [7, 2, 1, 1, 3, 18, 5, 1, 1, 6, 30, 8, 1, 1, 9, 42, 11, 1, 1, 12, 54, \ldots].$$

■

Capítulo 4

Unidades de campos cuadráticos

4.1. Conceptos básicos

Discutiremos algunos conceptos básicos, comenzaremos con el concepto de divisibilidad para cualquier anillo R conmutativo con identidad.

Sean $a, b \in R$, diremos que a divide a b (escribimos $a|b$) si existe algún $c \in R$ tal que $b = ac$. Cualquier divisor de 1 es llamado unidad. Decimos que a y b son *asociados* y lo denotamos por $a \sim b$ si existe una unidad $u \in R$ tal que $a = bu$, se verifica sin dificultad que $\sim$ es una relación de equivalencia.

Definición 4.1 *Sea R un anillo conmutativo con identidad. Si se cumple $\forall\ a, b, c \in R$ que: $a \cdot b = a \cdot c$ y $a \neq 0 \Longrightarrow b = c$ decimos que R es un dominio entero.*

Sea R un dominio entero y sean $a, b \neq 0$, tales que $a|b$ y $b|a$, tenemos entonces que a y b son asociados, pues existen $c, d \in R$ tales que $ac = b$ y $bd = a$, lo cual implica que $bcd = b$, como R es dominio entero, tenemos que $dc = 1$ y así d y c son unidades.

Decimos que $a \in R$ es *irreducible* si para cualquier factorización $a = bc$, se tiene que b ó c es unidad.

Sea R un dominio entero. Sea $n : R \longrightarrow \mathbb{N}$ una función tal que

(i) $n(ab) = n(a)n(b)\ \forall\ a, b \in R$, y

(ii) $n(a) = 1 \Longleftrightarrow a$ es unidad.

Llamamos a tal función una *función norma o norma* en R. Probaremos ahora que cuando se tiene una función norma en R, cada elemento $a \in R$ puede escribirse como producto de elementos irreducibles.

Sea $b \in R$, procedamos por inducción sobre la norma de b.

(1) Si b es irreducible, el resultado se tiene.

(2) Supongamos b no irreducible y el resultado válido para $b' \in R$ tal que $n(b') < n(b)$. Como b es no irreducible, entonces $b = ac$ donde $a, c \in R$, con a, c no unidades, luego por la condición (i)

$$n(b) = n(ac) = n(a)n(c)$$

y por la condición (ii), $n(a) < n(b)$ y $n(c) < n(b)$, si a y c son irreducibles terminamos, si no, como las normas son menores que la norma de b, por la hipótesis de inducción , los elementos considerados son producto de elementos irreducibles, y así b se descompone como producto de irreducibles.

Proposición 4.1 *Sea d libre de cuadrados. Considere*

$$R = \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}.$$

Entonces cada elemento de R puede escribirse como producto de irreducibles.

Demostración: Definimos la función $n : R \longrightarrow \mathbb{N}$, tal que para cada $a + b\sqrt{d} \in R$,

$$n(a + b\sqrt{d}) = |a^2 - db^2|.$$

Probaremos que la función definida anteriormente satisface las condiciones (i) y (ii), definidas anteriormente, en efecto:

(i) Sean $a+b\sqrt{d}, c+e\sqrt{d} \in R$, así

$$\begin{aligned} n[(a+b\sqrt{d})(c+e\sqrt{d})] &= n[(ac+bed)+(ae+bc)\sqrt{d}] \\ &= |(ac+bed)^2-(ae+bc)^2 d| \\ &= |(a^2-b^2d)(c^2-e^2d)| \\ &= n(a+b\sqrt{d})n(c+e\sqrt{d}) \end{aligned}$$

así la condición (i) se satisface.

(ii) Si $u=a+b\sqrt{d}$ es unidad en R, entonces existe $v=c+e\sqrt{d} \in R$ tal que $uv=1$. Pero por la condición (i), tenemos $1=n(1), 1=n(u)n(v)$. La función sólo toma valores enteros positivos, así $n(u)=n(v)=1$. Ahora si $n(u)=1$ entonces $u|1$ luego u es una unidad.

La función n satisface las condiciones requeridas, así cada elemento de R puede escribirse como producto de elementos irreducibles.

■

Ejemplo
Considere $R=\mathbb{Z}[\sqrt{-5}]$, aquí $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ son irreducibles en R y no son asociados. Observemos que:

$$6=2\cdot 3=(1-\sqrt{-5})(1+\sqrt{-5}),$$

así tenemos que en este caso en R, no se tiene una factorización única como producto de irreducibles.

Sea R un dominio entero, decimos que R es un *dominio de factorización única*, si satisface:

(i) Cada elemento de R distinto de cero y no unidad puede escribirse como producto de factores irreducibles, y

(ii) esta factorización es única, en el sentido de que si

$$a=\pi_1\cdots\pi_r \qquad \text{y} \qquad a=\tau_1\cdots\tau_s,$$

entonces $r=s$ y reenumerando en caso de ser necesario $\pi_i \sim \tau_i$.

La condición (ii), es equivalente a la siguiente condición:

(ii)* Si π es irreducible y π divide a ab, entonces $\pi|a$ ó $\pi|b$.

Sea R anillo. Un *ideal izquierdo (derecho)* I de R es un subgrupo aditivo de R tal que $RI \subseteq I$ $(IR \subseteq I)$.
Un *ideal* I de R es un ideal derecho e izquierdo.

Un ideal $I \subseteq R$ es llamado *principal* si puede ser generado por un sólo elemento de R. Un dominio R se dice *dominio de ideales principales*, si cada ideal de R es principal.

Sea R un anillo. Un ideal M de R se llama *maximal* si $M \neq R$ y si $M \subseteq I \subseteq R$ con I ideal entonces $I = M$ ó $I = R$.

Observación. Si π es un elemento irreducible en un dominio de ideales principales, entonces el ideal generado por (π) es maximal.

Teorema 4.2 *Si R es un dominio de ideales principales, entonces R es un dominio de factorzación única.*

Demostración: Sea S el conjunto de todos los elementos de R que no pueden escribirse como producto de irreducibles. Supongamos que $S \neq \phi$, sea $a_1 \in S$, como a_1 no es irreducible, podemos escribirlo como $a_1 = a_2 b_2$ donde ni a_2 ni b_2 son unidades. Entonces $(a_1) \subsetneqq (a_2)$ y $(a_1) \subsetneqq (b_2)$. Si suponemos que $a_2, b_2 \notin S$, entonces a_1 podría escribirse como producto de irreducibles. Suponemos así que $a_2 \in S$, procediendo inductivamente, obtenemos una cadena infinita de ideales

$$(a_1) \subsetneqq (a_2) \subsetneqq \cdots \subsetneqq (a_n) \subsetneqq \cdots$$

Consideremos ahora $I = \bigcup_{i=1}^{\infty}(a_i)$, este es un ideal de R, y como R es un dominio de ideales principales, $I = (\alpha)$ para algún $\alpha \in R$, entonces $\alpha \in I, \alpha \in (a_n)$ para algún n, pero entonces $(a_n) = (a_{n+1})$, y esto sería una contradicción, entonces $S = \phi$, se satisface así la condición (i) de la definición de dominio de factorización única.

Probaremos ahora la condición (ii)*, sea π un elemento irreducible tal que $\pi|ab$ para $a, b \in R$, si $\pi \not| a$, entonces el ideal $(a, \pi) = R$, así existen x, y tales que

$$ax + \pi y = 1 \Rightarrow abx + \pi by = b.$$

Entonces $\pi | abx$ y $\pi | \pi by$ así $\pi | b$, de lo anterior concluimos que R es un dominio de factorización única.

■

Definición 4.2 *Si R es un dominio entero, con una función (valuación o norma) $\phi : R \longrightarrow \mathbb{N}$ que satisface:*

(i) $\forall\ a, b \in R$ *con* $b \neq 0$, $\exists!\ q, r \in R$ *tales que* $a = bq + r$ *con* $r = 0$ *ó* $\phi(r) < \phi(b)$.

(ii) Sean a, b ambos no nulos, entonces $\phi(a) \leq \phi(ab)$.

R se llama dominio euclidiano.

La función ϕ es además multiplicativa, es decir

$$\forall\ a, b \in R, \phi(ab) = \phi(a)\phi(b)$$

Teorema 4.3 *Si el dominio R es euclidiano, entonces R es un dominio de ideales principales.*

Demostración: Sea $I \subseteq R$ un ideal, tomemos $a \in I$ tal que a sea un elemento de norma mínima en I. Sea $b \in I$, así obtenemos $q, r \in R$ tal que $b = aq + r$ donde $r = 0$ ó $\phi(r) < \phi(a)$. Pero $r = b - aq$ y así $r \in I$, como a es el elemento de norma mínima en I, tenemos $r = 0$, luego $b = aq$ para algún $q \in R$. Por lo tanto a es el generador de I, y R es un dominio de ideales principales.

■

Nota: Si $\mathbb{F}$ es un campo, entonces $\mathbb{F}[x]$, el anillo de polinomios en la indeterminada x con coeficientes en $\mathbb{F}$, es euclidiano.

Definición 4.3 *Un polinomio $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ se dice primitivo si el máximo común divisor de los coeficientes de $f(x)$ es 1. En particular un polinomio mónico es primitivo.*

El siguiente resultado, es conocido como *Lema de Gauss*:

Teorema 4.4 *Si R es un dominio de factorización única, y $f(x) \in R[x]$, definimos el contenido de f como el máximo común divisor de los coeficientes de f, denotado por $C(f)$. Para $f(x), g(x) \in R[x], C(fg) = C(f)C(g)$.*

Demostración: Considere dos polinomios $f(x), g(x) \in R[x]$, con $C(f) = c$ y $C(g) = d$, donde

$$f(x) = ca_0 + ca_1x + \cdots + ca_nx^n$$

y

$$g(x) = db_0 + db_1x + \cdots + db_mx^m,$$

donde $c, d, a_i, b_j \in R, a_n, b_m \neq 0$. Entonces $f = cf^*$ donde $f^* = a_0 + a_1x + \cdots + a_nx^n$, es un polinomio primitivo, y $g = dg^*$, con $g^* = b_0 + b_1x + \cdots b_mx^m$ un polinomio primitivo. Tenemos $fg = cd(f^*g^*)$, es suficiente demostrar que el producto de polinomios primitivos es primitivo. Sea

$$f^*g^* = k_0 + k_1x + \cdots + k_{m+n}x^{n+m},$$

y supongamos que este polinomio no es primitivo. Entonces todos los coeficientes k_i son divisibles por algún $\pi \in R$, con π irreducible. Como f^* y g^* son primitivos, entonces hay al menos un coeficiente de cada polinomio de f^* y de g^* que no es divisible por π. Sean a_i y b_j los primeros de tales coeficientes de f^* y g^*, respectivamente. Tenemos,

$$k_{i+j} = (a_0b_{i+j} + \cdots + a_{i-1}b_{j+1}) + a_ib_j + (a_{i+1}b_{j-1} + \cdots + a_{i+j}b_0)$$

Se tiene que $k_{i+j}, a_0, a_1, \ldots, a_{i-1}, b_0, b_1, \ldots, b_{j-1}$ son todos divisibles por π, así a_ib_j también es divisible por π, como π es irreducible, entonces $\pi | a_i$ o $\pi | b_j$, lo cual es una contradicción, probando con esto que f^*g^* es primitivo.

Finalmente, puesto que $fg = cdf^*g^*$, donde f^*g^* es primitivo, hemos demostrado que

$$C(fg) = cd = C(f)C(g).$$

■

4.2. Números algebraicos

Un número $\alpha \in \mathbb{C}$ se llama *número algebraico* si existe un polinomio

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

tal que $a_n, a_{n-1}, \ldots, a_0 \in \mathbb{Q}$ no todos nulos y $f(\alpha) = 0$. Si α es una raíz de un polinomio mónico con coeficientes en $\mathbb{Z}$, decimos que α es un *entero algebraico*. Claramente todos los enteros algebraicos son números algebraicos, el recíproco no es cierto.

Ejemplo

Demostraremos que $\dfrac{\sqrt{2}}{3}$ es un número algebraico, pero no es un entero algebraico. En efecto: consideremos el polinomio

$$f(x) = 9x^2 - 2 \in \mathbb{Q}[x], \text{ así } f\left(\frac{\sqrt{2}}{3}\right) = 0,$$

lo cual prueba que es número algebraico. Supongamos ahora que $\dfrac{\sqrt{2}}{3}$ es entero algebraico, entonces existe un polinomio mónico en $\mathbb{Z}[x]$, supongamos que tal polinomio es

$$g(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$$

tal que $\dfrac{\sqrt{2}}{3}$ es raíz, así

$$g\left(\frac{\sqrt{2}}{3}\right) = \left(\frac{\sqrt{2}}{3}\right)^n + b_{n-1}\left(\frac{\sqrt{2}}{3}\right)^{n-1} + \cdots + \left(\frac{\sqrt{2}}{3}\right) + b_0 = 0$$

entonces

$$(\sqrt{2})^n + b_{n-1}3(\sqrt{2})^{n-1} + \cdots + b_1 3^{n-1}(\sqrt{2}) + b_0 3^n = 0$$

si i es impar, $(\sqrt{2})^i$ no es entero, podemos separar nuestra ecuación en las siguientes ecuaciones

$$\sqrt{2}\sum_{i-impar} b_i 2^{(i-1)/2}3^{n-i} = 0, \qquad \sum_{i-par} b_i 2^{i/2}3^{n-i} = 0$$

para $i = 0, 1, \ldots, n$, como $3|0$, cada suma anterior debe ser divisible por 3. Cada sumando que contiene a b_i, $i \neq n$, tiene de factor a 3, así 3 divide al sumando que contiene a $b_n = 1$, obtenemos así que $3|2^{(n-1)/2}$ si n es impar, y $3|2^{n/2}$ si n es par. En cada caso esto es falso y concluimos así que $\dfrac{\sqrt{2}}{3}$ no es entero algebraico.

Observación:

i) Si $\alpha \in \mathbb{Q}$ es entero algebraico, entonces $\alpha \in \mathbb{Z}$.

ii) Si $4|d+1$, entonces $\dfrac{-1 \pm \sqrt{-d}}{2}$ es un entero algebraico.

Teorema 4.5 *Sea α un número algebraico. Entonces existe un único polinomio $p(x) \in \mathbb{Q}[x]$ mónico, irreducible y de grado mínimo tal que $p(\alpha) = 0$. Por lo tanto si $f(x) \in \mathbb{Q}[x]$ y $f(\alpha) = 0$, entonces $p(x)|f(x)$.*

Demostración: Consideremos

$$\mathcal{F} = \{p(x) : p(x) \in \mathbb{Q}[x] \;\; y \;\; p(\alpha) = 0\}$$

Sea $p(x) \in \mathcal{F}$ tal que su grado es mínimo, si $p(x)$ es no irreducible, sería producto de dos polinomios de menor grado en $\mathbb{Q}[x]$, es decir, $p(x) = a(x)b(x)$, así $p(\alpha) = a(\alpha)b(\alpha) = 0$, como $\mathbb{C}$ es un dominio entero, tendríamos $a(\alpha) = 0$ ó $b(\alpha) = 0$, lo cual contradice la minimalidad de $p(x)$, por lo tanto $p(x)$ debe ser irreducible. Probemos ahora la unicidad, sean $p(x)$ y $q(x)$ tales polinomios, aplicando el algoritmo de la división existen únicos $s(x), r(x) \in \mathbb{Q}[x]$ tales que

$$p(x) = s(x)q(x) + r(x) \text{ donde } r(x) = 0 \text{ ó grad } r(x) < \text{grad } q(x)$$

pero $p(\alpha) = s(\alpha)q(\alpha) + r(\alpha) = 0$ como $q(\alpha) = 0$, entonces $r(\alpha) = 0$, puesto que $p(x)$ y $q(x)$ son polinomios de grado mínimo para los cuales α es raíz, tenemos $r(x) = 0$, así $p(x) = s(x)q(x)$ y $s(x) \in \mathbb{C}^*$, entonces grad $p(x) =$

grad $q(x)$, luego $p(x)$ es único salvo una constante, podemos suponer así que el coeficiente principal es 1.

Finalmente sea $f(x) \in \mathbb{Q}[x]$ tal que $f(\alpha) = 0$, supongamos que $p(x)$ no divide a $f(x)$, puesto que $p(x)$ es irreducible, se tiene que $(f(x), p(x)) = 1$, luego existen $u(x), v(x) \in \mathbb{Q}[x]$ tales que

$$u(x)p(x) + v(x)f(x) = 1, \text{ luego } \quad u(\alpha)p(\alpha) + v(\alpha)f(\alpha) = 0 = 1$$

lo cual es una contradicción, así $p(x)|f(x)$.

■

El grado de $p(x)$ es llamado el grado de α y se denota por grad α, además $p(x)$ es llamado el polinomio mínimo de α. Los números complejos que no son *algebraicos* se denominan *trascendentes*.

4.3. Campos de números algebraicos

La teoría de campos de números algebraicos es muy vasta, en esta sección incluiremos los resultados y definiciones suficientes para el desarrollo del presente trabajo.

Teorema 4.6 *Sea α un número algebraico. Definimos*

$$\mathbb{Q}[\alpha] = \{f(\alpha) : f \in \mathbb{Q}[x]\}.$$

Entonces $\mathbb{Q}[\alpha]$ es un campo.

Demostración: Claramente $Q[\alpha]$ es un subanillo de $\mathbb{C}$. Sea f el polinomio mínimo de α, y consideremos el siguiente mapeo $\phi : \mathbb{Q}[x] \longrightarrow \mathbb{Q}[\alpha]$ definido por

$$\sum_{i=0}^{n} a_i x^i \longrightarrow \sum_{i=0}^{n} a_i \alpha^i$$

sin dificultad se verifica que $\phi(f + g) = \phi(f) + \phi(g), \phi(fg) = \phi(f)\phi(g)$, es decir ϕ es un homomorfismo, además Nucl $\phi = (f)$, el ideal generado por f. Aplicando uno de los teoremas de homomorfismos de anillos, obtenemos

$$\frac{\mathbb{Q}[x]}{(f)} \cong \mathbb{Q}[\alpha].$$

Sea g un polinomio en $\mathbb{Q}[x]$ tal que f no lo divide. Recordemos que $\mathbb{Q}[x]$ es un dominio euclidiano y por lo tanto es un dominio de ideales principales, luego el ideal generado por un irreducible es ideal maximal, luego $\mathbb{Q}[x]/(f)$ es un campo. Denotamos a $\mathbb{Q}[\alpha]$ por $\mathbb{Q}(\alpha)$.

■

El campo $\mathbb{F} \subseteq \mathbb{C}$ es llamado *campo de números algebraicos* si su dimensión sobre $\mathbb{Q}$ es finita. La dimensión de $\mathbb{F}$ sobre $\mathbb{Q}$ es llamada el *grado* de $\mathbb{F}$ y se denota por $[\mathbb{F} : \mathbb{Q}]$. Note que si α es un número algebraico de grado n, entonces $\mathbb{Q}(\alpha)$ es un *campo de números algebraicos* de grado n sobre $\mathbb{Q}$.

Sean α y β números algebraicos, $\mathbb{Q}(\alpha, \beta)$ es el campo que contiene a la intersección de todos los subcampos de $\mathbb{C}$ que contienen a $\mathbb{Q}, \alpha$ y β.

Presentamos el siguiente teorema cuya demostración queda fuera del alcanse de este trabajo, sin embargo ésta se ecuentra en[1].

Teorema 4.7 *(Teorema del elemento primitivo) Si α y β son números algebraicos, entonces existe un número algebraico θ, tal que $\mathbb{Q}(\theta) = \mathbb{Q}(\alpha, \beta)$.*

Este teorema puede generalizarse utilizando inducción, es decir: para el conjunto de números algebraicos $\alpha_1, \ldots, \alpha_n$, existe un número algebraico θ tal que

$$\mathbb{Q}(\alpha_1, \ldots, \alpha_n) = \mathbb{Q}(\theta).$$

Por lo tanto, cualquier campo de números algebraicos $\mathbb{F}$ es de la forma $\mathbb{Q}(\theta)$ para algún número algebraico θ.

Sea $p(x)$ el polinomio mínimo de α, entonces a las raíces del polinomio mínimo $p(x)$ se les llama *raíces conjugadas* o *conjugados* de α. Así, si n es el grado de $p(x)$, entonces α tiene n conjugados. Se verifica sin dificultad que si β es conjugado de α, entonces tienen el mismo polinomio mínimo.

[1] J. Esmonde, Problems in Algebraic Number Theory, Springer. pag. 31

Si $\theta = \theta^{(1)}$ y $\theta^{(2)}, \ldots, \theta^{(n)}$ son los conjugados de θ, entonces $\mathbb{Q}(\theta^{(i)})$ para $i = 2, \ldots, n$, es llamado el *campo conjugado* de $\mathbb{Q}(\theta)$, así el mapeo definido por $\theta \longrightarrow \theta^{(i)}$ es un monomorfismo $\mathbb{F} = \mathbb{Q}(\theta) \longrightarrow \mathbb{Q}(\theta^{(i)})$ (refiriéndonos a los encajes de $\mathbb{F}$ en $\mathbb{C}$). Se particionan los conjugados de θ en raíces reales y raíces no reales (llamadas raíces complejas).

El campo de números algebraicos $\mathbb{F}$ se llama *extensión normal* (o *extensión de Galois*) de $\mathbb{Q}$ si todos los campos conjugados de $\mathbb{F}$ son identicos a $\mathbb{F}$. Por ejemplo, cualquier extensión cuadrática de $\mathbb{Q}$ es normal, si consideramos a $\mathbb{Q}(\sqrt[3]{2})$, sus dos conjugados son $\mathbb{Q}(\zeta_3\sqrt[3]{2})$ y $\mathbb{Q}(\zeta_3^2\sqrt[3]{2})$, donde $\zeta_3 = \dfrac{-1+\sqrt{-3}}{2}$, y son distintos a $\mathbb{Q}(\sqrt[3]{2})$.

Se define la *cerradura normal* de cualquier campo $\mathbb{F}$ como la extensión $\overline{\mathbb{F}}$ de grado mínimo que contiene a todos los conjugados del campo $\mathbb{F}$. En el caso de $\mathbb{Q}(\sqrt[3]{2})$ su cerradura normal es $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$.

El siguiente teorema proporciona algunas caracterizaciones de los enteros algebraicos, los incisos 3 y 4 son utilizados más frecuentemente para verificar cuándo un número es entero algebraico o no.

Antes damos la siguiente:

Definición 4.4 *Sea R un anillo conmutativo con identidad. Un R-módulo (izquierdo) es un grupo aditivo abeliano M junto con una función*

$$\phi : R \times M \longrightarrow M$$

tal que $\forall\ r, s \in R$ *y* $\forall\ a, b \in M$
(i) $r(a+b) = ra + rb$
(ii) $(r+s)a = ra + rb$
(iii) $r(sa) = (rs)a$
(iv) $1a = a$.

Teorema 4.8 *Probaremos que las siguientes condiciones son equivalentes:*

1. *α es un entero algebraico.*

2. *El polinomio mínimo de α pertenece a $\mathbb{Z}[x]$.*
3. *$\mathbb{Z}[\alpha]$ es finitamente generado como $\mathbb{Z}-$módulo.*
4. *$\exists$ un $\mathbb{Z}$-módulo finitamente generado $M \neq \{0\}$ en $\mathbb{C}$ tal que $\alpha M \subseteq M$.*

Demostración: (1) $\Rightarrow$ (2) Sea $f(x)$ un polinomio mónico en $\mathbb{Z}[x]$ tal que $f(\alpha) = 0$. Sea $\phi(x)$ el polinomio mínimo de α.

Por el Teorema 4.5, tenemos que $f(x) = \phi(x)\psi(x)$, para algún $\psi(x) \in \mathbb{Q}[x]$, más aún

$$\phi(x) = \frac{a}{b}\phi_1(x),\ \phi_1(x) \text{ es primitivo, } a, b \in \mathbb{Z}, \phi_1(x) \in \mathbb{Z}[x],$$

$$\psi(x) = \frac{c}{d}\psi_1(x),\ \psi_1(x) \text{ es primitivo, } c, d \in \mathbb{Z}, \psi_1(x) \in \mathbb{Z}[x].$$

Así $bdf(x) = ac\phi_1(x)\psi_1(x)$. Por el *Lema de Gauss*, $\phi_1(x), \psi_1(x)$ y $f(x)$ son primitivos, así $bd = \pm ac$ y $f(x) = \pm\phi_1(x)\psi_1(x)$, entonces los coeficientes principales de los polinomios $\phi_1(x)$ y $\psi_1(x)$ son ± 1, por lo tanto $\phi(\alpha) = 0 \Rightarrow \phi_1(\alpha) = 0$, de esto $\phi(x) = \pm\phi_1(x)$ el cual es mónico en $\mathbb{Z}[x]$.

(2) $\Rightarrow$ (3) Sea $\phi(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ el polinomio mínimo de α. Además $\mathbb{Z}[\alpha] = \{f(\alpha) : f(x) \in \mathbb{Z}[x]\}$, para probar (3) basta obtener una base finita para $\mathbb{Z}[\alpha]$.

Probaremos que $\{1, \alpha, \ldots, \alpha^{n-1}\}$ genera a $\mathbb{Z}[\alpha]$ (como $\mathbb{Z}$-módulo). En efecto, para esto es suficiente demostrar que α^N, para cualquier $N \in \mathbb{Z}^+$, es una combinación lineal de $\{1, \ldots, \alpha^{n-1}\}$ con coeficientes en $\mathbb{Z}$. Procedamos por inducción, claramente la afirmación es válida para $N \leq n-1$. Para $N \geq n$, suponemos cierto para toda $\alpha^j, j < N$

$$\begin{aligned}
\alpha^N &= \alpha^{N-n} \cdot \alpha^n \\
&= \alpha^{N-n}[-(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1})] \\
&= (-\alpha^{N-n})a_0 + (-\alpha^{N-n}a_1)\alpha + \cdots + (-\alpha^{N-n}a_{n-1})\alpha^{n-1}.
\end{aligned}$$

Por la hipótesis inductiva, $-\alpha^{N-n}a_i \in \mathbb{Z}[\alpha],\ \forall\ i = 0, 1, \ldots, n-1$. Entonces $\mathbb{Z}[\alpha]$ es un $\mathbb{Z}$-módulo finitamente generado por $\{1, \alpha, \ldots, \alpha^{n-1}\}$.

(3) $\Rightarrow$ (4) Sea $M = \mathbb{Z}[\alpha]$. Claramente $\alpha\mathbb{Z}[\alpha] \subseteq \mathbb{Z}[\alpha]$.

(4) $\Rightarrow$ (1) Sean $x_1, \ldots, x_r$ generadores de M sobre $\mathbb{Z}$. Así

$$M = \mathbb{Z}x_1 + \mathbb{Z}x_2 + \cdots + \mathbb{Z}x_r$$

Por hipótesis $\alpha x_i \in M,\ \forall\ i = 1, 2, \ldots, r$, existe un conjunto de $c_{ij} \in \mathbb{Z}$ tal que

$$\alpha x_i = \sum_{j=1}^{n} c_{ij}\, x_i,\ \ \forall\, i = 1, 2, \ldots, r.$$

Entonces

$$C \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} = \alpha \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} \iff (C - \alpha I) \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} = 0$$

Tenemos que $x_1, \ldots, x_r$ no son todos nulos, luego $\det(C - \alpha I) = 0$. En otras palabras,

$$\begin{vmatrix} c_{11} - x & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} - x & \cdots & c_{2n} \\ & & & \\ c_{n1} & c_{n2} & \cdots & c_{nn} - x \end{vmatrix} = 0, \text{ cuando } x = \alpha.$$

Éste es una ecuación polinomial en $\mathbb{Z}[x]$ de grado n cuyo coeficiente principal es $(-1)^n$, de donde

$$f(x) = \begin{cases} \det(C - xI) & n \text{ es par} \\ \\ -\det(C - xI) & n \text{ es impar} \end{cases}$$

Entonces $f(x)$ es un polinomio mónico en $\mathbb{Z}[x]$ tal que $f(\alpha) = 0$, así α es entero algebraico.

■

Teorema 4.9 *Sea $\mathbb{F}$ un campo de números algebraicos. Sea $\mathcal{O}_{\mathbb{F}}$ el conjunto de todos los enteros algebraicos de $\mathbb{F}$. Entonces $\mathcal{O}_{\mathbb{F}}$ es un anillo.*

Demostración: Sean α, β enteros algebraicos, por el teorema anterior $\mathbb{Z}[\alpha], \mathbb{Z}[\beta]$ son finitamente generados como $\mathbb{Z}$-módulos. Así $M = \mathbb{Z}[\alpha, \beta]$ es también finitamente generado como $\mathbb{Z}$-módulo, más aún

$$(\alpha \pm \beta)M \subseteq M, \qquad (\alpha\beta)M \subseteq M.$$

Así $\alpha \pm \beta$ y $\alpha\beta$ son enteros algebraicos, es decir $\alpha \pm \beta$ y $\alpha\beta$ pertenecen $\mathcal{O}_{\mathbb{F}}$, por lo tanto $\mathcal{O}_{\mathbb{F}}$ es un anillo.

■

4.4. Unidades en campos cuadráticos

Sean $\mathbb{F}$ un campo de números y $\mathcal{O}_{\mathbb{F}}$ el anillo de enteros. Un elemento $\alpha \in \mathcal{O}_{\mathbb{F}}$ es llamado *unidad* si existe $\beta \in \mathcal{O}_{\mathbb{F}}$ tal que $\alpha\beta = 1$. Evidentemente, el conjunto de todas las unidades en $\mathcal{O}_{\mathbb{F}}$ forman un subgrupo multiplicativo de $\mathbb{F}^*$, el cual se llama el grupo de unidades de $\mathbb{F}$, denotado por $\mathcal{U}_{\mathbb{F}}$.

Definición 4.5 *$\alpha \in \mathcal{O}_{\mathbb{F}}$ se llama una raíz de unidad si existe $m \in \mathbb{N}$ tal que $\alpha^m = 1$.*

Sea $\mathbb{F}$ un campo cuadrático. Puede probarse sin dificultad, que la función $N : \mathbb{F} \longrightarrow \mathbb{R}$ definida por:

$$N(\alpha) = \alpha\bar{\alpha}$$

donde $\bar{\alpha}$ denota al conjugado de α, es una norma.
Consideraremos el siguiente resultado, que no probaremos, sin embargo su demostración puede encontrarse en[2].

Proposición 4.10 *Un entero algebraico α es unidad si, y sólo si su norma es $N(\alpha) = \pm 1$.*

[2]Ribenboim Paulo, Algebraic Number, Ed. Wiley-Interscience 1972, pag. 76

El estudio de los campos numéricos está en la base de la teoría algebraica de números, en nuestro caso nos restringiremos al caso de los *campos cuadráticos*, es decir, los campos numéricos de grado 2. Comencemos describiendo a estos campos.
Si $\mathbb{F}$ es un campo cuadrático, la teoría de Galois nos garantiza la existencia de un elemento primitivo, es decir, existe $\zeta \in \mathbb{F}$ tal que $\mathbb{F} = \mathbb{Q}(\zeta)$, entonces el polinomio mínimo de ζ tiene grado 2, multiplicándolo por una constante obtenemos un polinomio $ax^2 + bx + c$ con coeficientes enteros y raíz ζ y $a \neq 0$. Si llamamos $D = b^2 - 4ac$, entonces $\zeta = \dfrac{-b \pm \sqrt{D}}{2a}$, y es claro que $\mathbb{F} = \mathbb{Q}(\sqrt{D})$.

El número D no puede ser un cuadrado perfecto, o de lo contrario $\mathbb{F} = \mathbb{Q}$ y su grado sería 1. Digamos que $D = m^2 d$, donde d es libre de cuadrados (quizá $d = -1$). Entonces $\sqrt{D} = m\sqrt{d}$ y es evidente que $\mathbb{F} = \mathbb{Q}(\sqrt{d})$. En resumen todo campo cuadrático es de la forma $\mathbb{Q}(\sqrt{d})$ para un entero d libre de cuadrados, así

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}.$$

Como cada elemento de $\mathbb{F}$ es de la forma $a + b\sqrt{d}$, su conjugado es $a - b\sqrt{d}$, tenemos así lo siguiente:

Teorema 4.11 *Sea $\mathbb{F}$ un campo cuadrático, así $\mathbb{F} = \mathbb{Q}(\sqrt{d})$, con d libre de cuadrados. Sea $\mathcal{O}_\mathbb{F}$ el anillo de enteros algebraicos. Entonces:*

1. $a + b\sqrt{d} \in \mathcal{O}_\mathbb{F} \iff 2a = u \in \mathbb{Z}, 2b = v \in \mathbb{Z}$ *y* $u^2 - dv^2 \equiv 0 \mod 4$.
2. *Si* $d \not\equiv 1 \mod 4$, *entonces* $\mathcal{O}_\mathbb{F} = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$. *Si* $d \equiv 1 \mod 4$, *entonces* $\mathcal{O}_\mathbb{F} = \left\{\dfrac{u}{2} + \dfrac{v}{2}\sqrt{d} : u, v \in \mathbb{Z}, u \text{ y } v \text{ tienen la misma paridad}\right\}$.
3. *Si* $d \not\equiv 1 \mod 4$, *entonces* $\{1, \sqrt{d}\}$ *es base de* $\mathcal{O}_\mathbb{F}$, *y así* $\mathcal{O}_\mathbb{F} = \mathbb{Z}[\sqrt{d}]$. *Si* $d \equiv 1 \mod 4$, *entonces* $\left\{1, \dfrac{1 + \sqrt{d}}{2}\right\}$ *es base de* $\mathcal{O}_\mathbb{F}$, *y obtenemos así* $\mathcal{O}_\mathbb{F} = \mathbb{Z}\left[\dfrac{1 + \sqrt{d}}{2}\right]$.

Demostración:

1. Si $x = a + b\sqrt{d} \in \mathcal{O}_{\mathbb{F}}$, entonces su conjugado $\overline{x} = a - b\sqrt{d}$ es tambien un entero algebraico, así $x + \overline{x} = 2a \in \mathcal{O}_{\mathbb{F}} \cap \mathbb{Q} = \mathbb{Z}$, tenemos además que $x \cdot \overline{x} = a^2 - db^2 \in \mathcal{O}_{\mathbb{F}} \cap \mathbb{Q} = \mathbb{Z}$.

   Se sigue que $(2a)^2 - (2b)^2 d \in 4\mathbb{Z}$. Como $(2a)^2 \in \mathbb{Z}$, tenemos $(2b)^2 d \in \mathbb{Z}$, pero como d es libre de cuadrados, $2b$ tiene denominador igual a 1, así que $v = 2b \in \mathbb{Z}$. Recíprocamente, las condiciones implican $a^2 - db^2 \in \mathbb{Z}$, y x es raíz de $x^2 - 2ax + (a^2 - db^2)$, entonces x es entero algebraico.

2. Examinemos todos los posibles casos en la sucesión:

   a) Si $d \equiv 2 \mod 4$, entonces

u	par	par	impar	impar	
v	par	impar	par	impar	
$u^2 - dv^2$	0	2	1	3	mod 4

   b) Si $d \equiv 3 \mod 4$, entonces

u	par	par	impar	impar	
v	par	impar	par	impar	
$u^2 - dv^2$	0	1	1	2	mod 4

   c) Si $d \equiv 1 \mod 4$, entonces

u	par	par	impar	impar	
v	par	impar	par	impar	
$u^2 - dv^2$	0	3	1	0	mod 4

3. La conclusión es obvia, cuando $d \not\equiv 1 \mod 4$. Consideraremos así el caso en que $d \equiv 1 \mod 4$, probaremos que cada entero algebraico $\frac{u}{2} + \frac{v}{2}\sqrt{d}$ (con u, v enteros de la misma paridad), es una combinación lineal de 1 y $\frac{1+\sqrt{d}}{2}$, con coeficientes en $\mathbb{Z}$.

   Si u y v son pares, es decir $u = 2a, v = 2b$ con $a, b \in \mathbb{Z}$, así

$$\frac{u}{2} + \frac{v}{2}\sqrt{d} = a + b\sqrt{d} = (a-b)1 + 2b\left(\frac{1+\sqrt{d}}{2}\right).$$

   Si u, v son impares, entonces $u-1$ y $v-1$ son pares, así

$$\frac{u}{2} + \frac{v}{2}\sqrt{d} = \left(\frac{1+\sqrt{d}}{2}\right) + \left(\left[\frac{u-1}{2}\right] + \left[\frac{v-1}{2}\right]\sqrt{d}\right),$$

   el último sumando de la expresión anterior es una combinación lineal de $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$, con coeficientes en $\mathbb{Z}$.

■

Teorema 4.12 *Consideramos $\mathbb{Q}(\sqrt{d})$, con $d < 0$ y libre de cuadrados, las unidades están caracterizadas de la siguiente forma: si $d \neq -1, d \neq -3$, entonces las unidades de $\mathbb{Q}(\sqrt{d})$ son $1, -1$. Las unidades de $\mathbb{Q}(\sqrt{-1})$ son $1, -1, i, -i$. Para $\mathbb{Q}(\sqrt{-3})$, las unidades son $1, -1, \frac{1+\sqrt{-3}}{2}, \frac{1-\sqrt{-3}}{2}, \frac{-1+\sqrt{-3}}{2}, \frac{-1-\sqrt{-3}}{2}$.*

En este caso, cada unidad es una raíz de unidad.

Demostración: Si $d \equiv 2 \mod 4$ ó $d \equiv 3 \mod 4$, entonces los enteros de $\mathbb{Q}(\sqrt{d})$ son de la forma $x = a + b\sqrt{d}$, con $a, b \in \mathbb{Z}$; el conjugado de x es de la forma $x' = a - b\sqrt{d}$ y la norma es $N(x) = xx' = a^2 - db^2$. Como x es unidad,

es necesario y suficiente que $N(x) = \pm 1$, así basta hallar las soluciones de $a^2 - db^2 = 1$ con $d < 0$.

Las únicas posibles soluciones son $a = \pm 1, b = 0$, excepto cuando $d = -1$, en cuyo caso también se tienen las soluciones $a = 0, b = \pm 1$.

Si $d \equiv 1 \mod 4$, los enteros de $\mathbb{Q}(\sqrt{d})$ son de la forma $x = \dfrac{a + b\sqrt{d}}{2}$, con $a, b \in \mathbb{Z}$ y tienen la misma paridad, procediendo como antes, se obtiene que el problema se reduce a hallar las soluciones de $a^2 - b^2 d = 4$, así las únicas posibles soluciones son $a = \pm 2, b = 0$, excepto en el caso $d = -3$, donde tenemos otras soluciones $a = \pm 1, b = \pm 1$. Estas unidades corresponden a las seis raíces de unidad.

■

Consideraremos ahora el caso en que $d > 0$, así $\mathbb{Q}(\sqrt{d})$ está contenido en el campo de los números reales, así sus únicas raíces de unidad son 1 y -1, sin embargo hay más unidades en $\mathbb{Q}(\sqrt{d})$.

Teorema 4.13 *Sea n el periodo de la fracción continua $\sqrt{d}$.*

1. *Todas las soluciones enteras de la ecuación $x^2 - dy^2 = \pm 1$ están dadas por*
$$x + y\sqrt{d} = \pm(p_{n-1} + q_{n-1}\sqrt{d})^l \ : \ l \in \mathbb{Z}$$
donde p_{n-1}/q_{n-1} es el $(n-1)$-ésimo convergente de la fracción continua $\sqrt{d}$.

2. *Si d es libre de cuadrado, $d \equiv 2, 3 \mod 4$, entonces $p_{n-1} + q_{n-1}\sqrt{d}$ es unidad fundamental de $\mathbb{Q}(\sqrt{d})$.*

3. *La ecuación $x^2 - dy^2 = -1$ posee solución entera si y solo si n es impar.*

4. *Si d tiene un divisor primo $p \equiv 3 \mod 4$, entonces la ecuación $x^2 - dy^2 = -1$ no tiene solución entera.*

Demostración:

1. Cualquier solución (x, y) está descrita por la ecuación

$$(x + \sqrt{d}y)^{-1} = \pm(x - \sqrt{d}y)$$

Por lo tanto una de $\pm(a, \pm b)$ es solución de $x^2 - dy^2 = \pm 1$ y cada uno de los cuatro pares es solución. Es suficiente que mostremos que todas las soluciones positivas están dadas por

$$x + y\sqrt{d} = (p_{n-1} + q_{n-1}\sqrt{d})^m \, , m < 0.$$

Por el Teorema 2.8, si $x^2 - dy^2 = \pm 1$, entonces $x = p^{k-1}, y = q_{k-1}$, para algún k. Probemos ahora que, si d es un entero positivo libre de cuadrados, y $\alpha = \alpha_0 = \sqrt{d}$, entonces

$$p_{k-1}^2 - dq_{k-1}^2 = (-1)^k Q_k,$$

para todo $k \geq 1$, entonces p_k/q_k es el k-ésimo convergente de la fracción continua α y Q_k se define como en el Teorema 2.10. En efecto, por inspección, $p_0^2 - dq_0^2 = [\sqrt{d}]^2 - d = -Q_1$. Ahora supongamos que $k \geq 2$. Escribimos

$$\sqrt{d} = \alpha_0 = [a_0, a_1, \ldots, a_{k-1}, \alpha_k] = \frac{\alpha_k p_{k-1} + p_{k-2}}{\alpha_k q_{k-1} + q_{k-2}}.$$

Como $\alpha_k = (P_k + \sqrt{d})/Q_k$, tenemos

$$\sqrt{d} = \frac{(P_k + \sqrt{d})p_{k-1} + Q_k p_{k-2}}{(P_k + \sqrt{d})q_{k-1} + Q_k q_{k-2}},$$

luego $dq_{k-1} + (P_k q_{k-1} + Q_k q_{k-2})\sqrt{d} = P_k p_{k-1} + Q_k p_{k-2} + p_{k-1}\sqrt{d}$
Ecuación con coeficientes en $\mathbb{Q}(\sqrt{d})$, tenemos

$$dq_{k-1} = P_k p_{k-1} + Q_k p_{k-2}$$

y

$$p_{k-1} = P_k q_{k-1} + Q_k q_{k-2}.$$

Así

$$p_{k-1}^2 - dq_{k-1}^2 = (p_{k-1}q_{k-2} - p_{k-2}q_{k-1})Q_k = (-1)^k Q_k.$$

Por lo anterior, $p_{k-1}^2 - dq_{k-1}^2 = (-1)^k Q_k = \pm 1 \;\Rightarrow\; Q_k = \pm 1$ y esto implica que $n|k$, entonces

$$p_{n-1} < p_{2n-1} < \cdots \quad \text{y} \quad q_{n-1} < q_{2n-1} < \cdots,$$

tenemos en particular, que la mínima solución positiva dada por la ecuación es $x_1 = p_{n-1}, y_1 = q_{n-1}$. Mostremos ahora que todas las soluciones positivas (x_m, y_m) están dadas por $x_m + y_m\sqrt{d} = (x_1 + y_1\sqrt{d})^m,\ m > 0$. Tomando los $\mathbb{Q}$-conjugados, $x_m - y_m\sqrt{d} = (x_1 - y_1\sqrt{d})^m$

$$(x_m + y_m\sqrt{d})(x_m - y_m\sqrt{d}) = (x_1^2 - dy_1^2)^m = (\pm 1)^m = \pm 1,$$

así (x_m, y_m) es solución. Evidentemente, $x_1 < x_m, y_1 < y_m$, así que (x_m, y_m) es una solución positiva.

Ahora supongamos que (X, Y) es una solución positiva y que no es una de (x_m, y_m). Entonces existe un entero $\kappa \geq 0$ tal que

$$(x_1 + y_1\sqrt{d})^\kappa < X + Y\sqrt{d} < (x_1 + y_1\sqrt{d})^{\kappa+1},$$

o

$$1 < (x_1 + y_1\sqrt{d})^{-\kappa}(X + Y\sqrt{d}) < x_1 + y_1\sqrt{d}.$$

Pero $x_1^2 - dy_1^2 = \pm 1$, lo cual implica que

$$(x_1 + y_1\sqrt{d})^{-\kappa} = [\pm(x_1 - y_1\sqrt{d})]^\kappa.$$

Definamos los enteros s, t tales que

$$s + t\sqrt{d} = (x_1 + y_1\sqrt{d})^{-\kappa}(X + Y\sqrt{d}) = \pm(x_1 - y_1\sqrt{d})^\kappa(X + Y\sqrt{d}).$$

Entonces

$$s^2 - dt^2 = [\pm(x_1 - y_1\sqrt{d})^\kappa(X + Y\sqrt{d})][\pm(x_1 + y_1\sqrt{d})^\kappa(X - Y\sqrt{d})]$$

$$= X^2 - dY^2 = \pm 1.$$

Así (s, t) es solución de la ecuación con $1 < s + t\sqrt{d} < x_1 + y_1\sqrt{d}$.

También,

$$0 < (x_1 + y_1\sqrt{d})^{-1} < (s + t\sqrt{d})^{-1} < 1 < s + t\sqrt{d}.$$

Pero esto implica que

$$2s = s + t\sqrt{d} \pm [\pm(s - t\sqrt{d})] = s + t\sqrt{d} \pm (s + t\sqrt{d})^{-1} > 0$$

$$2t\sqrt{d} = s + t\sqrt{d} \pm [\pm(s - t\sqrt{d})] > 0,$$

y así (s, t) es una solución positiva. Por hipótesis, entonces $s \geq x_1, t \geq y_1$ y, entonces $s + t\sqrt{d} < x_1 + y_1\sqrt{d}$, y tenemos una contradicción.

2. Entonces de (1), se sigue inmediatamente que $p_{n-1} + q_{n-1}\sqrt{d} > 1$.

3. $x^2 - dy^2 = -1 \Rightarrow x = p_{k-1}, y = q_{k-1}$ para algún k, por el Teorema 2.8. Pero $p_{k-1}^2 - dq_{k-1}^2 = (-1)^k Q_k$ si y sólo si $n|k$ y k es impar. Claramente esta solución existe si y sólo si n es impar.

4. $x^2 - dy^2 = -1$ implica que $x^2 \equiv -1 \mod p$, para todo $p|d$. Pero para $p \equiv 3 \mod 4$, esta congruencia no tiene solución.

■

Tenemos los siguientes ejemplos:

Ejemplos.

1. La fracción simple de $\sqrt{6}$ es, utilizando la notación del Teorema 2.10, tomando $\alpha = \alpha_0 = \sqrt{6}$, tenemos

$P_0 = 0,$	$P_1 = 2,$	$P_2 = 2,$
$Q_0 = 1,$	$Q_1 = 2,$	$Q_2 = 1,$
$\alpha_0 = \sqrt{6},$	$\alpha_1 = \dfrac{2 + \sqrt{6}}{2},$	$\alpha_2 = 2 + \sqrt{6},$
$a_0 = 2,$	$a_1 = 2,$	$a_2 = 4,$

Así, el periodo de la fracción continua α es 2, entonces $\sqrt{6} = [a_0, \overline{a_1, a_2}] = [2, \overline{2, 4}]$. Un procedimientno ánalogo nos permite obtener que la fracción continua de $\sqrt{23} = [4, \overline{1, 3, 1, 8}]$.

2. Utilizando el Teorema 4.13 parte (2), calculemos las unidades fundamentales de $\mathbb{Q}(\sqrt{6})$ y $\mathbb{Q}(\sqrt{23})$. Para $\sqrt{6}$,

$$C_1 = \frac{p_1}{q_1} = [a_0, a_1] = a_0 + \frac{1}{a_1} = 1 + \frac{1}{2} = \frac{5}{2}$$

así la unidad fundamental en $\mathbb{Q}(\sqrt{6})$ es $5 + 2\sqrt{6}$.

Para $\sqrt{23}, C_3 = [4, 1, 3, 1] = 24/5$. Por lo tanto la unidad fundamental en $\mathbb{Q}(\sqrt{23})$ es $24 + 5\sqrt{23}$.

3. Veamos ahora que $[d, \overline{2d}]$ es la fracción continua de $\sqrt{d^2 + 1}$. Observemos que

$$d^2 < d^2 + 1 < (d + 1)^2 \ \ \forall\, d > 0,$$

tenemos así que $[\![\sqrt{d^2 + 1} \ ]\!] = d$ y tomando $\alpha = \alpha_0 = \sqrt{d^2 + 1}$, tenemos

$$\begin{aligned} P_0 &= 0, & P_1 &= d, \\ Q_0 &= 1, & Q_1 &= 1, \\ \alpha_0 &= \sqrt{d^2 + 1}, & \alpha_1 &= d + \sqrt{d^2 + 1}, \\ a_0 &= d, & a_1 &= 2d, \end{aligned}$$

Esto implica que el periodo de la fracción continua $\sqrt{d^2 + 1}$ es 1, por lo tanto

$$\sqrt{d^2 + 1} = [a_0, \overline{a_1}] = [d, \overline{2d}].$$

4. Concluyamos ahora que si $d^2 + 1$ es libre de cuadrados y $d \equiv 1, 3 \mod 4$, entonces la unidad fundamental de $\mathbb{Q}(\sqrt{d^2 + 1})$ es $d + \sqrt{d^2 + 1}$.

Si $d \equiv 1, 3 \mod 4$ y así $d^2 + 1 \equiv 2 \mod 4$. Entonces, si $d^2 + 1$ es libre de cuadrado, la unidad fundamental de $\mathbb{Q}(\sqrt{d^2 + 1})$ es $p_0 + q_0\sqrt{d^2 + 1} = d + \sqrt{d^2 + 1}$. Con esto se puede calcular de manera muy fácil las unidades fundamentales de $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{10}), \mathbb{Q}(\sqrt{26})$.

5. Veamos ahora que la fracción continua de $\sqrt{d^2+2}$ es $[d, \overline{d, 2d}]$. Observemos que

$$d^2 < d^2 + 2 < (d+1)^2 \ \ \forall\, d \geq 1$$

tenemos $[\![\ \sqrt{d^2+2}\ ]\!] = d$ y sea $\alpha = \alpha_0 = \sqrt{d^2+2}$, tenemos

$$\begin{aligned}
&P_0 = 0,\\
&Q_0 = 1,\\
&\alpha_0 = \sqrt{d^2+2},\\
&a_0 = d,\\
&P_1 = d,\\
&Q_1 = 2,\\
&\alpha_1 = \frac{d+\sqrt{d^2+2}}{2},\\
&a_1 = d,\\
&P_2 = d,\\
&Q_2 = 1,\\
&\alpha_2 = d + \sqrt{d^2+2},\\
&a_2 = 2d,
\end{aligned}$$

Por lo tanto el periodo de la fracción continua de $\sqrt{d^2+2}$ es 2, así

$$\sqrt{d^2+2} = [a_0, \overline{a_1, a_2}] = [d, \overline{d, 2d}]$$

así

$$\frac{p_1}{q_1} = d + \frac{1}{d} = \frac{d^2+1}{d}$$

Considere ahora d^2+1 libre de cuadrados, entonces las unidades fundamentales de $\mathbb{Q}(\sqrt{d^2+2})$, quedan descritas por:

como para todo d, $d^2+2 \equiv 2, 3 \mod 4$, la unidad fundamental es

$$p_1 + q_1\sqrt{d^2+2} = d^2 + 1 + d\sqrt{d^2+2}$$

con lo anterior se calculan de manera muy simple las unidades para $\mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{11}), \mathbb{Q}(\sqrt{51}), \mathbb{Q}(\sqrt{66})$.

■

Conclusiones

El método de fracciones continuas, cuyo principo básico utiliza el conocido *algoritmo de euclides*, tiene un vasto campo de aplicación, cabe observar que éste fué uno de los métodos más conocidos en en siglo $XVII$, siendo una de sus aplicaciones hallar soluciones de ciertas ecuaciones diofantinas.

Una aplicación inmediata que se tiene del método de fracciones continuas es el concerniente a la obtención de la expresión del máximo común divisor de dos enteros como una combinación lineal de éstos (se encuentran una infinidad de soluciones y no solo una como la que se obtiene de la aplicación inmediata del algoritmo de la división para dos enteros), ya que lo anterior se reduce a encontrar las soluciones de una ecuación diofantina lineal en dos variables.

Otras de sus aplicaciones es que al tratar de obtener soluciones de ciertas ecuaciones diofantinas, éste involucra procedimientos que permiten calcular unidades fundamentales de campos cuadráticos, siendo éste un algoritmo simple y eficiente.

Como mencionamos anteriormente las fracciones continuas tienen una gran diversidad de aplicaciones, basta comentar que se utilizan para obtener sucesiones recurrentes, métodos de factorización, pruebas de primalidad, juegos de salón, por mencionar algunas.

Como un hecho curioso, se tiene que la sucesión de Fibonacci y el número áureo, se relacionan vía las fracciones continuas.

Bibliografía

[1] Burton W. Jones, *Teoría de los números*, Biblioteca de matemática superior, Ed. Trillas.

[2] C.D Olds Zanicheli, *Frazioni Continue*, MMS.

[3] Carlos Ivorra Castillo, *Teoría de Números*, www.uv.es/∽ivorra/Libros/Numeros.pdf

[4] Courant-Robbins, *Qué son las matemáticas?*, Ed. Fondo de cultura económica.

[5] Dummit-Foote, *Abstract Algebra*, Ed. John Wiley & Sons, Inc.

[6] J. Esmonde, *Problems in Algebraic Number Theory*, Springer.

[7] John B. Fraleigh, *Álgebra Abstracta*, SITESA Addison-Wesley, Iberoamericana.

[8] N.N. Vorobyov, *Temas matemáticos, los números de Fibonacci*, Ed. Limusa.

[9] Ribenboim Paulo, *Algebraic Number*, Ed. Wiley-Interscience, 1972.