Universidad de Valladolid
Facultad de Ciencias

TRABAJO FIN DE GRADO

Grado en Matemáticas

Fracciones continuas. La ecuación de Pell

Autor: Daniel Nieto Medina

Tutor: Félix Delgado de la Mata

Índice general

Introducción

El tema central de este trabajo son las fracciones continuas y como utilizarlas en la resolución de ecuaciones diofánticas, en nuestro caso, especialmente en la conocida ecuación de Pell. Lo primero que se piensa cuando se habla de matemáticas es en los números, sin duda ellos constituyen, junto con la geometría, el origen y fundamento de las matemáticas. Las fracciones continuas permiten una representación de los números reales alternativa a su expresión decimal y mucho más ligada a propiedades de algebraicidad, por ejemplo los irracionales cuadráticos (es decir, los que son raíz de una ecuación racional de segundo grado) se expresan como una fracción continua periódica.

A lo lago de la historia grandes matemáticos han contribuido al desarrollo de la teoría de fracciones continuas y las han usado como instrumento en la resolución de ecuaciones diofánticas o como medio de aproximar números reales, citemos entre ellos a Cataldi, Bombelli, Euler, Lagrange, Lambert, Gauss. De hecho ya Euclides en el año 300 a.c. usaba las fracciones continuas de manera implicita aunque no es hasta los años entorno al 1500 en que Cataldi y Bombeli desarrollan su uso y estudian sus propiedades. Posteriormente, cabe destacar el uso que tuvieron en la demostración de la trascendencia de π. Actualmente se usan, por ejemplo, en las expansiones de Engel, que usa las fracciones continuas de manera ascendente (numerador) y no como haremos en este trabajo de manera descendente (denominador). A pesar de que pueda parecer un mecanismo obsoleto y en desuso en la actualidad ello no es cierto, la sencillez de sus ideas y la potencia de su técnica hace que se esté extendiendo su uso en dimensiones mayores, en contextos geométricos, en problemas de factorización útiles en criptografía, en teoría de grupos o en otros objetos algebraicos como los anillos de series de potencias.

En nuestro caso el uso de las fracciones continuas se encuadra en un problema clásico de teoría de números: el problema de la factorización en anillos de números, más concretamente de anillos cuadráticos. El problema de replicar el Teorema fundamental de la aritmética en anillos de números es un problema ligado de forma inequívoca al nacimiento del álgeba moderna. El hecho de que dichos anillos no sean factoriales llevó en su momento a Dedekind a introducir la noción de ideal como extensión del concepto de número y a probar que para ideales sí se tiene factorización. El cálculo de las unidades (elementos inversibles para el producto) de los anillos cuadráticos es, en este contexto, un problema natural cuya resolución lleva al uso de las fracciones continuas. Es este planteamiento el que hemos adoptado en esta memoria para introducir y desarrollar las fracciones continuas.

El primer capítulo está dedicado a marcar el contexto, el campo de juego, es decir desarrolla la teoría básica de los cuerpos y anillos cuadráticos, Nos centrare-

mos especialmente en las propiedades ligadas a la factorización, por lo tanto tendrán especial interés los conceptos de dominio de ideales principales, euclídeos y de factorización única. Restringiéndonos a este último caso, junto con la caracterización de los elementos irreducibles, el cálculo de la las unidades es la pieza fundamental. Sobre todo en los cuerpos cuadráticos reales, que tienen infinitas unidades, y son considerablemente más complicadas de calcular que en el caso de los anillos cuadráticos complejos en donde el número de unidades es finito.

Para poder encontrar dichas unidades tendremos que trabajar con la norma de un elemento y se plantea el problema de resolver ecuaciones del tipo

$$x^2 - dy^2 = \pm 1 \ ,$$

es decir, de la ecuación de Pell. Es aquí donde entra en juego el uso de las fracciones continuas, tema al que se dedica el segundo capítulo de la memoria. Además de las propiedades estándar el capítulo se cierra con el Teorema de Lagrange que caracteriza los números cuadráticos como aquellos cuya fracción continua es periódica.

El último capítulo retoma el problema del cálculo de las unidades de los anillos de números cuadráticos mediante el uso de los convergentes de la fracción continua de $\sqrt{d}$. Los resultados que precisan la aproximación de un irracional a partir de sus convergentes, que es uno de los aspectos fundamentales de la teoría de fracciones continuas, juegan en este caso un papel importante.

Puesto que se trata de un tema clásico y de uso universal en teoría de números las fuentes bibliográficas son muy amplias: prácticamente la totalidad de los libros de teoría elemental de números incluyen algún tema de fracciones continuas. En nuestro caso para el tratamiento de las fracciones continuas nos hemos apoyado sobre todo en dos referencias clásicas, el libro de LeVeque [4] y el de Olds, [5]. No obstante, en conjunto nuestra fuente principal ha sido una referencia mucho más moderna, el libro de Hill [3], cuyo planteamiento es mucho más acorde con el que nosotros hemos adoptado.

Capítulo 1

Cuerpos Cuadráticos

En este capítulo haremos un estudio de las extensiones cuadráticas de $\mathbb{Q}$ y, sobre todo, de sus anillos de enteros. Además de una rápida revisión de los resultados estándar de teoría de cuerpos necesarios, el objetivo principal es establecer los resultados principales de los anillos de números cuadráticos desde el punto de vista de la factorización. El hecho de que el Teorema fundamental de la aritmética no sea válido en anillos de enteros como es bien sabido está en la base de la introducción de la noción de ideal por Dedekind y de la prueba de que la factorización sigue siendo cierta si sustituimos números por ideales. En el caso de las extensiones cuadráticas nos limitamos a probar la descomposición de los números primos en el caso en que el anillo de enteros es un dominio de factorización única. Este hecho, junto con el cálculo de la unidades del anillo permite describir la descomposición de cualquier elemento del anillo en una vía semejante a la del caso de los enteros.

1.1. Introducción y primeros resultados

Sean K, L dos cuerpos tales que K es un subcuerpo de L, decimos en este caso que $K \subseteq L$ es una extensión de cuerpos. También se denota por L/K. Se define el grado de la extension como la dimensión de L considerado como espacio vectorial sobre el cuerpo K. Se denota $[L : K]$. Si $[L : K]$ es finito se dice que la extension es finita.

Sea $K \subset L$ una extensión, si $\alpha \in L$, $K[\alpha]$ denota el anillo de expresiones polinómicas en α:

$$K[\alpha] = \{P(\alpha) = a_0 + a_1\alpha^1 + \ldots + a_n\alpha^n \quad : \quad P(x) = \sum_{i=1}^{n} a_i x^i \in K[x]\} .$$

$K[\alpha]$ es el mínimo subanillo de L que contiene a K y a α. Su cuerpo de fracciones es

$$K(\alpha) = \{P(\alpha)/Q(\alpha) \quad : \quad P(x), Q(x) \in K[x], Q(\alpha) \neq 0\} ,$$

que es un subcuerpo de L, $K \subset K(\alpha) \subset L$, de hecho el menor subcuerpo que contiene a K y a α.

Definición 1. Un número complejo α se dice que es un número algebraico si existe un polinomio $P(x) \in \mathbb{Q}[x]$ tal que $P(\alpha) = 0$.

Su polinomio mínimo es el (único) polinomio $P(x)$ mónico de grado mínimo tal que $P(\alpha) = 0$.

El polinomio mínimo $P(x)$ de un número algebraico α es irreducible en $\mathbb{Q}[x]$ y el conjunto de polinomios que se anulan en α es el ideal principal generado por $P(x)$:

$$\{Q(x) \in \mathbb{Q}[x] \quad : \quad Q(\alpha) = 0\} = (P(x)) \ .$$

Proposición 1. *Sea $\alpha \in \mathbb{C}$, son equivalentes:*

1) $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$

2) α *es algebraico.*

3) $[\mathbb{Q}[\alpha] : \mathbb{Q}]$ *es finita.*

Además, si α es algebraico y $P(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ con $a_0, \ldots, a_{n-1} \in \mathbb{Q}$ es su polinomio mínimo se tiene que :

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \ldots - a_1\alpha - a_0$$

por lo que α^n es una combinación lineal sobre $\mathbb{Q}$ de $1, \alpha, \ldots, \alpha^{n-1}$. Si multiplicamos por α en la igualdad y sustituimos el término α^n, obtendremos α^{n+1} como combinación lineal sobre $\mathbb{Q}$ de $1, \alpha, \ldots, \alpha^{n-1}$. Continuando el proceso podemos ver que cada polinomio sobre $\mathbb{Q}$ en α se puede reducir a un polinomio sobre $\mathbb{Q}$ en α de grado menor que n. De hecho $\{1, \alpha, \ldots, \alpha^{n-1}\}$ es una base de $\mathbb{Q}(\alpha)$ sobre $\mathbb{Q}$.

Sea $\alpha \in \mathbb{C}$ algebraico y $K = \mathbb{Q}(\alpha)$ y sea $P(x)$ su polinomio mínimo. Dicho polinomio tiene n raíces complejas (incluyendo a α), $\alpha, \alpha_1, \ldots, \alpha_{n-1}$, se dice que $\alpha_1, \ldots, \alpha_{n-1}$ son los conjugados de α. Se llama norma de α al producto de sus conjugados $N(\alpha) = \alpha\alpha_1 \ldots \alpha_{n-1}$. La norma de α es un número racional, ya que si $P(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ con $a_{n-1}, \ldots, a_0 \in \mathbb{Q}$, $N(\alpha) = (-1)^n a_0$.

La suma de su conjugados $Tr(\alpha) = \alpha + \alpha_1 + \ldots + \alpha_{n-1}$ se llama traza de α y es también un número racional, de hecho $Tr(\alpha) = -a_{n-1}$.

1.2. Cuerpos cuadráticos

Definición 2. Llamaremos cuerpo cuadrático a un subcuerpo K de $\mathbb{C}$ de grado 2 sobre $\mathbb{Q}$.

Diremos que un entero d es libre de cuadrados si a^2 no divide a d para cada entero $a \neq \pm 1$, o equivalentemente, si no tiene factores primos al cuadrado en su factorización como producto de primos. En lo sucesivo d siempre denotará un entero libre de cuadrados.

Observación 1. Sea K un cuerpo cuadrático. Si $\alpha \in \mathbb{Q} \subset K$ entonces su polinomio mínimo es $x - \alpha$. Tomemos $\alpha \in K \setminus \mathbb{Q}$, entonces $\{1, \alpha\}$ es una $\mathbb{Q} - base$ de K, en particular $K = \mathbb{Q}(\alpha)$. Como $\alpha^2 \in K$ existen coeficientes $q, r \in \mathbb{Q}$ tales que

$$\alpha^2 = q\alpha + r$$

o, equivalentemente $p(\alpha) = 0$ si $p(x) = x^2 - qx - r$. Nótese que $P(x)$ es el polinomio mínimo de α.

Proposición 2. *Todos los cuerpos cuadráticos son de la forma:*

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

con d libre de cuadrados. Mas aún, si $\mathbb{Q}(\sqrt{d})$ *y* $\mathbb{Q}(\sqrt{d'})$ *son isomorfos, entonces* $d = d'$.

Demostración. Dado $d \in \mathbb{Z}$ libre de cuadrados, fácilmente podemos ver que $\mathbb{Q}(\sqrt{d})$ es un cuerpo cuadrático. Sean K un cuerpo cuadrático y $\alpha \in K \setminus \mathbb{Q}$, entonces $K = \mathbb{Q}(\alpha)$. Como $[K : \mathbb{Q}] = 2$ tenemos que $1, \alpha, \alpha^2$ son linealmente dependientes, por lo tanto existen $a, b, c \in \mathbb{Q}$ tales que $a \neq 0$ y $a\alpha^2 + b\alpha + c = 0$. Sin perdida de generalidad, podemos suponer que $a, b, c \in \mathbb{Z}$. Multiplicando por $4a$ tenemos que:

$$(2a\alpha + b)^2 = b^2 - 4ac$$

Denotemos $\beta = 2a\alpha + b$ y $n = b^2 - 4ac \in \mathbb{Z}$. Luego $\mathbb{Q}(\sqrt{n}) \subset \mathbb{Q}(\beta)$ y $\mathbb{Q}(\beta) = K$. Además $[\mathbb{Q}(\sqrt{n}) : \mathbb{Q}] = 2$ por lo que $K = \mathbb{Q}(\sqrt{m})$ donde $n = k^2 m$ con $m \in \mathbb{Z}$ libre de cuadrados.

□

Sea $K = \mathbb{Q}(\sqrt{d})$ un cuerpo cuadrático, el conjunto de conjugados de $\sqrt{d}$ es $\{\sqrt{d}, -\sqrt{d}\}$, usaremos el término "conjugado de $\sqrt{d}$ " para nombrar a $-\sqrt{d}$. Sea $\alpha \in K \setminus \mathbb{Q}$, $\alpha = a + b\sqrt{d}$, tenemos que $(a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2 \in \mathbb{Q}$ y $(a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a \in \mathbb{Q}$. Por lo tanto, si $\overline{\alpha}$ es la única raíz conjugada de α,distinta de α, es $\overline{\alpha} = a - b\sqrt{d}$. Además, como $N(\alpha) = \alpha\overline{\alpha} = a^2 - db^2$, $Tr(\alpha) = 2a$, su polinomio mínimo será

$$P(x) = (x + \alpha)(x - \overline{\alpha}) = x^2 - Tr(\alpha)x + N(\alpha) \qquad (*)$$

Definición 3. Un número complejo α se dice que es un entero algebraico si es raíz de un polinomio mónico en $\mathbb{Z}[x]$.

Llamaremos O_K al conjunto de los enteros algebraicos de un cuerpo cuadrático K. Es claro que $O_K \bigcap \mathbb{Q} = \mathbb{Z}$. Para $\alpha \in \mathbb{C}$ denotaremos

$$\mathbb{Z}[\alpha] = \{p(\alpha) \in \mathbb{C} : p(x) \in \mathbb{Z}[x]\}.$$

Nótese que $\mathbb{Z}[\alpha]$ es el mínimo subanillo de $\mathbb{C}$ que contiene a $\mathbb{Z}$ y a α.

Definición 4. Sea d un entero libre de cuadrados ($d \neq 0, 1$). Definimos el entero algebraico $\alpha = \alpha_d$ como sigue:

$$\alpha_d = \begin{cases} \sqrt{d} & \text{si } d \equiv 2, 3 \bmod 4 \\ \dfrac{1 + \sqrt{d}}{2} & \text{si } d \equiv 1 \bmod 4 \end{cases} \qquad (1.1)$$

Nótese que si $d \equiv 2, 3 \bmod 4$, entonces $\alpha = \sqrt{d}$ que es una raíz de $p(x) = x^2 - d$. Si $d \equiv 1 \bmod 4$, tenemos $(\alpha - 1/2)^2 = d/4$, por tanto $\alpha^2 + \frac{1}{4} - \alpha = \frac{d}{4}$. Esto implica, $p(\alpha) = 0$ donde $p(x) = x^2 - x + \dfrac{1 - d}{4}$. Como $d \equiv 1 \bmod 4$, $\frac{1-d}{4}$ es entero y por tanto α es un entero algebraico.

Teorema 1. *Sea $K = \mathbb{Q}(\sqrt{d})$. Entonces:*

$$O_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & si\ d \equiv 2, 3\ mod 4 \\ \mathbb{Z}\Big[\dfrac{1+\sqrt{d}}{2}\Big] & si\ d \equiv 1\ mod\ 4 \end{cases} \tag{1.2}$$

Demostración. Si $\beta = r + s\sqrt{d} \in K \setminus \mathbb{Q}$, su polinomio esta dado por $(*)$. Por tanto β es un entero algebraico si y sólo si $Tr(\beta) = 2r \in \mathbb{Z}$ y $N(\beta) = r^2 - ds^2 \in \mathbb{Z}$. Puesto que $2r \in \mathbb{Z}$, entonces o bien $r \in \mathbb{Z}$ o $r = \frac{r_1}{2}$con r_1 impar. Si tenemos que $r \in \mathbb{Z}$, la condición $r^2 - ds^2 \in \mathbb{Z}$ implica que $ds^2 \in \mathbb{Z}$ y, como d es libre de cuadrados, forzosamente $s \in \mathbb{Z}$.

Si $r = \frac{r_1}{2}$ con r_1 impar, la condición $\frac{r_1}{4} - ds^2 \in \mathbb{Z}$ equivale a $r_1^2 - 4ds^2 \in 4\mathbb{Z}$. Obsérvese que en este caso $s \notin \mathbb{Z}$, y que si $s \in \mathbb{Z}$ tendríamos que $r_1^2 \in 4\mathbb{Z}$, lo que es absurdo pues r_1 impar y por lo tanto $r_1 \equiv 1 \bmod 4$. Por tanto $s = \frac{a}{b}$ con $m.c.d(a, b) = 1$, $b \neq 1$. La condición $4d\frac{a^2}{b^2} \in \mathbb{Z}$ implica que $b = 2$, ya que d libre de cuadrados. Así pues, $r = \frac{r_1}{2}$, $s = \frac{a}{2}$ con r_1, a impares. Nótese que en este caso, $r_1^2 \equiv 1 \bmod 4$ y $a^2 \equiv 1 \bmod 4$ de manera que

$$\frac{r_1}{4} - d\frac{a^2}{4} \in \mathbb{Z} \Leftrightarrow r_1^2 - da^2 \in 4\mathbb{Z} \Leftrightarrow r_1^2 \equiv da^2 \quad mod \quad 4 \Leftrightarrow d \equiv 1 \quad mod \quad 4.$$

Por tanto el caso $r = \frac{r_1}{2}$, $s = \frac{a}{2}$ con r_1, a impares solo se puede dar si $d \equiv 1 \bmod 4$.

□

Llamaremos a $\mathbb{Z}[\alpha]$, $\alpha = \alpha_d$, un anillo cuadrático. Si $d > 0$, entonces los elementos de $\mathbb{Z}[\alpha]$ son números reales, y diremos que $\mathbb{Z}[\alpha]$ es un anillo cuadrático real. Si $d < 0$ en $\mathbb{Z}[\alpha]$ hay elementos complejos no reales, diremos que $\mathbb{Z}[\alpha]$ es un anillo cuadrático complejo.

Ejemplo 1. Si $d = -1$, como $-1 \not\equiv 1 \bmod 4$, tenemos $\alpha = \sqrt{-1}$. En este caso el anillo cuadrático es $\mathbb{Z}[i]$. A este anillo se le conoce como el anillo de los enteros de Gauss.

Si $d = -3$, como $-3 \equiv 1 \bmod 4$, tenemos

$$\alpha = \frac{1+\sqrt{-3}}{2} = \frac{1}{2} + i\frac{\sqrt{3}}{2} = \cos(\frac{2\pi}{6}) + i\sin(\frac{2\pi}{6}) = e^{\frac{2\pi i}{6}}.$$

Este anillo se llama anillo de los enteros de Eisenstein. El polinomio mínimo de α es $x^2 - x + 1$, y como $(x^2 - x + 1)(x + 1) = (x^3 + 1)$, $(x^3 + 1)(x^3 - 1) = x^6 - 1$, α es la raíz sexta fundamental de la unidad.

1.3. Conjugados normas y unidades

Ya hemos visto cómo se definen las normas y el conjugado. Sea $\beta = a + b\sqrt{d}$ en $\mathbb{Q}(\sqrt{d})$, tendremos $\overline{\beta} = a - b\sqrt{d}$ y $N(a + b\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2\sqrt{d}$.

Si $d \equiv 1 \bmod 4$, tenemos $\alpha = \alpha_d = \dfrac{1+\sqrt{d}}{2}$, y $\overline{\alpha} = \dfrac{1-\sqrt{d}}{2} = 1 - \alpha$, además

$$N\Big(a+b\frac{1+\sqrt{d}}{2}\Big)=\Big(a+\frac{b}{2}\Big)^2-d\Big(\frac{b}{2}\Big)^2=a^2+ab+\Big(\frac{1-d}{4}\Big)b^2.$$

Si $d\equiv 2,3 \bmod 4$, $\alpha=\sqrt{d}$ y $\overline{\alpha}=-\sqrt{d}=-\alpha$. Se tendrá entonces que $N(a+b\sqrt{d})=a^2-b^2d$.

En todo caso vemos que la norma de un elemento de $\mathbb{Z}[\alpha]$ es un entero, y la norma de un elemento de $\mathbb{Q}(\sqrt{d})$ un número racional.

Lema 1 (**Propiedades de los conjugados**). *Para todo elemento $A,B\in\mathbb{Q}(\sqrt{d})$ tenemos:*

1. $\overline{AB}=\overline{A}\,\overline{B}$, $\overline{A+B}=\overline{A}+\overline{B}$ *y* $\overline{\overline{A}}=A$.

2. *Si* $A\in\mathbb{Z}[\alpha]$, *entonces* $\overline{A}\in\mathbb{Z}[\alpha]$.

3. $N(AB)=N(A)N(B)$. *Si* $N(A)=0$, *entonces* $A=0$.

La demostración de este lema son operaciones elementales con las expresiones
$A=x_1+y_1\sqrt{d}$,
$B=x_2+y_2\sqrt{d}$.

Definición 5. Una unidad de un anillo es un elemento con inverso para la multiplicación. Las unidades se llaman también elementos invertibles del anillo.

El conjunto de unidades del anillo R se denota por R^* y es un grupo con la aplicación multiplicación.

Proposición 3. *Un elemento $A\in\mathbb{Z}[\alpha]$ es una unidad si y solo si $N(A)=\pm 1$.*

Demostración. Si $N(A)=\pm 1$, entonces $A\overline{A}=\pm 1$ y $A^{-1}=\overline{A}$ si $N(A)=1$ y $A^{-1}=-\overline{A}$ si $N(A)=-1$, y ambos son elementos de $\mathbb{Z}[\alpha]$.
Si A es invertible entonces $N(A)N(A^{-1})=N(AA^{-1})=N(1)$, por lo tanto $N(A)$ es factor de 1, por lo que $N(A)=\pm 1$.

□

Si $d<0$, es decir si $\mathbb{Q}(\sqrt{d})$ es una extesión cuadrática compleja, se tiene $\sqrt{d}=i\sqrt{|d|}$ y si $A=a+b\sqrt{d}$, $\overline{A}=a-b\sqrt{d}=a-bi\sqrt{|d|}$ es su complejo conjugado. Por tanto $N(A)=|A|^2$ y las unidades del anillo $\mathbb{Z}[\alpha]$ están en el círculo unidad.

Ejemplo 2. En el anillo de los enteros de Gauss $\mathbb{Z}[i]$, tenemos $\overline{x+iy}=x-iy$. Por lo tanto,

$$N(x+iy)=(x+iy)(x-iy)=x^2+y^2$$

Para encontrar unidades, necesitamos encontrar todas las soluciones enteras a $x^2+y^2=1$. Estas soluciones son $x=\pm 1$, $y=0$ y $x=0$, $y=\pm 1$. Entonces, las unidades en $\mathbb{Z}[i]$ son $1,-1,i$ y $-i$.

Ejemplo 3. Vamos a encontrar las unidades en el anillo de los enteros de Eisenstein. En este caso, $\alpha = \dfrac{1+\sqrt{-3}}{2} = e^{2\pi i/6}$, y tenemos $N(x+y\alpha) = x^2 + xy + y^2$. Por tanto, para encontrar las unidades, debemos encontrar todas las soluciones enteras a $x^2 + xy + y^2 = 1$.

Completando cuadrados en esta ecuación tenemos

$$\left(x + \frac{1}{2}y\right)^2 + \frac{3}{4}y^2 = 1$$

Esto nos da que $y^2 \leq \frac{4}{3}$. Como y es un entero, esto implica que $|y| \leq 1$. De manera similar obtenemos que $|x| \leq 1$. Si $y = 0$, entonces debemos tener $x = \pm 1$, y si $y = \pm 1$ entonces $x^2 + xy + 1 = 1$, por tanto $x = 0, -y$ son soluciones ambas. Esto nos da seis soluciones:

$$(1,0), (-1,0), (0,1), (0,-1), (1,-1), (-1,1)$$

Cada solución corresponde a una unidad, por tanto las unidades en los enteros de Eisenstein son:

$$1, -1, \alpha, -\alpha, -1+\alpha, 1-\alpha$$

Generalizando estos ejemplos, tenemos una descripción completa de todas las unidades en los anillos cuadráticos complejos:

Teorema 2. *Sea d un entero libre de cuadrados, $d < 0$, y sea $\mathbb{Z}[\alpha]$ el correspondiente anillo cuadrático complejo. Entonces las unidades en $\mathbb{Z}[\alpha]$ son:*

$$\mathbb{Z}[\alpha]^* = \begin{cases} \{1, -1, i, -i\} & \textit{si d=-1} \\ \{1, -1, \alpha, -\alpha, 1-\alpha, \alpha - 1\} & \textit{si d=-3} \\ \{1, -1\} & \textit{en otro caso} \end{cases} \tag{1.3}$$

Demostración. Los casos $d = -1, -3$ ya los vimos en los ejemplos. Supongamos $d < 0$, $d \neq -1, -3$.

Supongamos primero que $d \not\equiv 1 \bmod 4$. Entonces tenemos $N(a+b\alpha) = a^2 - db^2$, por tanto tenemos que encontrar solución a la ecuación $a^2 - db^2 = 1$.

Notese que $-d > 1$ por lo que debemos tener $b = 0$ y $a = \pm 1$. Las dos soluciones (-1,0), (1,0) dan dos unidades 1 y -1.

Asumiremos ahora que $d \equiv 1 \bmod 4$, se tiene $(d \neq -3)$ que $d \leq -7$ y por tanto tenemos que encontrar soluciones a la ecuación

$$a^2 + ab + \frac{1-d}{4}b^2 = 1$$

Completando cuadrados tenemos:

$$\left(a + \frac{1}{2}b\right)^2 - \frac{d}{4}b^2 = 1$$

Como $\frac{-d}{4} > 1$, tenemos $b = 0$. Esto implica $a = \pm 1$ como en el primer caso.

□

Hemos encontrado todas las unidades en cada anillo cuadrático complejo. En cada caso el grupo $\mathbb{Z}[\alpha]^*$ es finito.

Veamos ahora el caso de los cuerpos cuadráticos reales. Para ello enunciaremos el Teorema de Dirichlet para aproximaciones diofánticas:

Teorema 3. *(***Dirichlet***)*
Sea γ un número irracional y Q un entero mayor que 1. Entonces existen enteros p y q, con $1 \leq q \leq Q$ tal que

$$\left|\gamma - \frac{p}{q}\right| \leq \frac{1}{qQ}$$

Demostración. Consideremos los $Q+1$ número reales

$$q\gamma - \lfloor q\gamma \rfloor \text{ con } q = 0, \ldots, Q$$

(siendo $\lfloor x \rfloor$ la parte entera de x). Como γ es irracional, estos son $Q+1$ números distintos en el intervalo [0,1]. Dividiendo el intervalo en Q subintervalos de longitud $1/Q$, el principio del palomar asegura que podemos encontrar dos enteros $0 \leq q_1 < q_2 \leq Q$ tal que

$$|(q_1\gamma - \lfloor q_1\gamma \rfloor) - (q_2\gamma - \lfloor q_2\gamma \rfloor)| \leq \frac{1}{Q}$$

Por lo tanto

$$\left|\frac{\lfloor q_2\gamma \rfloor - \lfloor q_1\gamma \rfloor}{q_2 - q_1} - \gamma\right| \leq \frac{1}{(q_2 - q_1)Q}$$

Tomamos entonces $p = \lfloor q_2\gamma \rfloor - \lfloor q_1\gamma \rfloor$ y $q = q_2 - q_1 \leq Q$.

□

Teorema 4. *El anillo de enteros de un cuerpo cuadrático real tiene infinitas unidades.*

Demostración. Basta demostrar que cuando $d > 0$, hay una unidad η en $\mathbb{Z}(\sqrt{d})$ distinta de ± 1, porque entonces η^m es una unidad para todo entero m. En este caso, puesto que las únicas raíces de la unidad en $\mathbb{Q}(\sqrt{d})$ son ± 1, vemos que diferentes m dan unidades distintas.

Usaremos el teorema de Dirichlet para $\gamma = \sqrt{d}$. Sabemos que para cualquier entero $Q > 1$, existen enteros racionales p, q con $1 \leq q \leq Q$ tal que $|\beta| \leq \frac{1}{Q}$ con $\beta = p - q\sqrt{d}$.

Para cada $Q = 1, 2, 3, \ldots$ fijamos un elemento $\beta_Q \in \mathbb{Z}[\sqrt{d}]$ con estas condiciones, en particular $|N(\beta_Q)| < 3\sqrt{d}$. Puesto que $\sqrt{d}$ es irracional, $\beta_Q \neq \beta_{Q'}$ si $Q \neq Q'$. Por lo tanto tenemos infinitos elementos $\{\beta_Q\}$ con $|N(\beta_Q)| < 3\sqrt{d}$, y como $|N(\beta_Q)| \in \mathbb{N}$ hay una subsucesión infinita que toma siempre el mismo valor, es decir, existe $N \in \mathbb{N}$, $N < 3\sqrt{d}$ tal que $|N(\beta_Q)| = N$ para infinitos Q.

El número de clases residuales módulo N es finito, por tanto existen dos elementos $\beta_Q = p - q\sqrt{d}$, $\beta_{Q'} = p' - q'\sqrt{d}$ tales que $|N(\beta_Q)| = |N(\beta_{Q'}| = N$ y $p \equiv p' \bmod N$,

$q \equiv q' \bmod N$. Sea además $\eta = \frac{\beta_Q}{\beta_{Q'}} \in \mathbb{Q}(\sqrt{d})$. Tenemos $|N(\eta)| = \dfrac{|N(\beta_Q)|}{|N(\beta'_Q)|} = \frac{N}{N} = 1$, y claramente $\eta \neq \pm 1$, ya que $\sqrt{d}$ es irracional y q, q' positivos.

$$\eta = \frac{p - q\sqrt{d}}{p' - q'\sqrt{d}} = \frac{(p - q\sqrt{d})(p' + q'\sqrt{d})}{p'^2 - q'^2 d} = \frac{pp' - qq'd - (p'q - pq')\sqrt{d}}{N}.$$

Tenemos que $p' = p + lN$, $q' = q + kN$ con $l, k \in \mathbb{Z}$, por tanto:

$$\begin{aligned} pp' - qq'd &= p(p + lN) - q(q + kN)d \\ &= p^2 - q^2 d + (pl - qkd)N \\ &= \pm N + (pl - qkd)N \equiv 0 \qquad \text{mód} \quad N \end{aligned}$$

y $x = \frac{pp' - qq'd}{N} \in \mathbb{Z}$. De la misma forma $y = \frac{pq' - p'q}{N} \in \mathbb{Z}$ y por lo tanto:

$$\eta = x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$$

Si $d \not\equiv 1 \bmod 4$, $\mathbb{Z}[\sqrt{d}] = \mathbb{Z}[\alpha]$ y si $d \equiv 1 \bmod 4$ tenemos que $\mathbb{Z}[\sqrt{d}] \subset \mathbb{Z}[\alpha]$ por lo que también $\mathbb{Z}[\alpha]$ tiene infinitas unidades.

□

Observación 2. Observemos que si $a, b \in \mathbb{N}$, entonces $\beta = a + b\sqrt{d} \geq 0$. De hecho $\beta > 1$ salvo que $\beta = 0$ o $\beta = 1 + 0 \cdot \sqrt{d} = 1$. Por lo tanto, si $\eta = k + l\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, $\eta \neq 0, \pm 1$ se tiene que $\{\pm\eta, \pm\overline{\eta}\} = \{\pm k \pm l\sqrt{d}\}$ y hay exactamente un elemento de dicho conjunto mayor que 1, $|k| + |l|\sqrt{d}$. En particular, por el Teorema anterior tenemos que existe una unidad en $\mathbb{Z}[\sqrt{d}]$, $\eta = a + b\sqrt{d}$, con $a, b \geq 0$ y $\eta > 1$.

Como consecuencia, el conjunto $U_\eta = \{\eta \in \mathbb{Z}[\alpha]^* \quad : \eta > 1\}$ es no vacío. Puesto que, si $\eta = a + b\sqrt{d} \in \mathbb{Z}[\alpha]$ entonces o bien $(a, b) \in \mathbb{Z}\text{x}\mathbb{Z}$ o $(a, b) \in \mathbb{Z}\text{x}\mathbb{Z} + (\frac{k}{2}, \frac{l}{2})$, el conjunto de elementos de U_η menos que en un entero fijo k es finito. Por lo tanto existe el mínimo elemento de U_η, $\varepsilon = \min U_\eta$. La unidad $\varepsilon \in \mathbb{Z}[\alpha]$ es la mínima unidad de $\mathbb{Z}[\alpha]$ mayor que 1. La llamamos la unidad fundamental de $\mathbb{Z}[\alpha]$.

Corolario 1. *El conjunto de unidades de $\mathbb{Z}[\alpha]$ es el conjunto infinito:*

$$\{\pm\varepsilon^m \ : \ m \in \mathbb{Z}\}$$

Demostración. Sea $\beta > 1$ una unidad de $\mathbb{Z}[\alpha]$ y $m \geq 0$ tal que $\varepsilon^m < \beta \leq \varepsilon^{m+1}$. El cociente $\frac{\beta}{\varepsilon^m}$ es también una unidad de $\mathbb{Z}[\alpha]$, $1 < \frac{\beta}{\varepsilon^m} \leq \varepsilon$ y por la definición de ε, $\frac{\beta}{\varepsilon^m} = \varepsilon$, es decir, $\beta = \varepsilon^m$. El caso general se deduce de forma parecida, ya que si $\beta \in \mathbb{Z}[\alpha]^*$ uno de los elementos $\{\pm\beta, \pm\frac{1}{\beta}\}$ es mayor que 1.

□

Nota 1. Si $d \equiv 1 \ \bmod 4$ sabemos que $\mathbb{Z}[\sqrt{d}] \neq \mathbb{Z}[\alpha]$. La observación anterior se puede establecer también para las unidades del anillo $\mathbb{Z}[\sqrt{d}]$, que es un subgrupo del grupo de unidades de $\mathbb{Z}[\alpha]$. Es decir, si $\eta \in \mathbb{Z}[\sqrt{d}]^*$, $\eta > 1$ es la unidad más pequeña, entonces $\mathbb{Z}[\sqrt{d}]^* = \{\pm\eta^n \ : \ n \in \mathbb{Z}\}$.

1.4. Anillos cuadráticos de norma Euclídea

Definición 6. Sea A un dominio de integridad, tenemos las siguientes definiciones:

-Un elemento $\gamma \in A$ se llama irreducible si es no nulo, no es una unidad y $\gamma = a \cdot b$ implica que a o b es una unidad.

-A se dice de factorización si todo elemento γ no nulo y no unidad, puede escribirse como $\gamma = \gamma_1 \dots \gamma_n$ con $\gamma_1, \dots, \gamma_n$ elementos irreducibles.

-A se dice dominio de factorización única (DFU) si es de factorización y además si $\gamma = \gamma_1 \dots \gamma_n = \delta_1 \dots \delta_m$ (γ_i, δ_i irreducibles) entonces $n = m$ y existe una permutación s de n elementos tal que γ_i es asociado a $\delta_{s(i)}$ para todo i (esto es, existe ε_i unidad tal que $\varepsilon_i \gamma_i = \delta_{s(i)}$).

-A se dice dominio de ideales principales (DIP) si todo ideal de A es principal, es decir, generado por un elemento.

-A se dice dominio Euclídeo (DE) si existe $\varphi : A \setminus \{0\} \longrightarrow \mathbb{N}$ tal que

1. Si $a, b \in A \setminus \{0\}$ entonces $\varphi(a) \leq \varphi(ab)$.
2. Si $a, b \in A$ y $b \neq 0$ entonces existen $q, r \in A$ tales que $a = bq + r$ donde $r = 0$ o $r \neq 0$ y $\varphi(r) < \varphi(a)$.

Es bueno recordar que:

$$DE \Rightarrow DIP \Rightarrow DFU \Rightarrow DF$$

Proposición 4. *Sea $\mathbb{Z}[\alpha]$ un anillo cuadrático y $\gamma \in \mathbb{Z}[\alpha]$, $\gamma \neq 0$. Entonces γ se factoriza como producto de irreducibles en $\mathbb{Z}[\alpha]$.*

Demostración. Si $\gamma \in \mathbb{Z}[\alpha]$ no es nulo ni unidad, tiene un divisor irreducible γ_1. Esto se demuestra por inducción, de manera que si γ fuese irreducible concluiríamos, si no lo fuese podríamos escribir $\gamma = ab$ con $N(\gamma) > N(a)$. Si a es irreducible acabamos y si no lo es continuaríamos con el proceso y llegaríamos a un divisor irreducible debido a que las norma son números naturales y acabaríamos teniendo norma mínima, debido a que cada divisor tiene norma estrictamente menor que su dividendo. Entonces $\gamma = \gamma_1 a_1$ con $1 \leq N(a_1) < N(\gamma)$. Si a_1 no es irreducible y no es unidad ($N(a_1) \neq 1$), entonces $a_1 = \gamma_2 a_2$, con γ_2 irreducible, obteniendo así una sucesión de números naturales $N(\gamma), N(a_1), N(a_2), \dots$ la cual en algún momento debe estabilizarse en 1, digamos $N(a_j) = 1$. Por lo tanto, $\gamma = \gamma_1 \dots \gamma_j a_j$ con $\gamma_1, \dots, \gamma_{j-1}, \gamma_j$ elementos irreducibles, y a_j unidad.

□

Ejemplo 4. Sea $K = \mathbb{Q}(\sqrt{-14})$, $O_K = \mathbb{Z}[\sqrt{-14}]$ su anillo de enteros. Veamos que el ideal $I = 2O_K + \sqrt{-14}O_K = (2, \sqrt{-14})$ no es principal. Supongamos que $I = aO_K$ para algún $a \in O_K$. Tenemos que $a|2$ entonces existe $b \in O_K$ tal que $2 = ab$. Tomando norma a ambos lados obtenemos que $4 = N(a)N(b)$. De la misma forma, como $a\big|\sqrt{-14}$ resulta que $N(a)$ divide a $N(\sqrt{-14}) = 14$, por lo tanto $N(a)$ es 1 o 2. Escribiendo $a = x + y\sqrt{-14}$ tenemos que $N(a) = x^2 + 14y^2 \neq 2$, entonces $N(a) = 1$ y se tiene $I = aO_K = O_K$ lo cual no es cierto.

Como consecuencia el anillo cuadrático $\mathbb{Z}[\sqrt{-14}]$ no es un DIP.

De hecho $\mathbb{Z}[\sqrt{-14}]$ no es un DFU. En efecto

$$3^4 = 81 = (5 + 2\sqrt{-14})(5 - 2\sqrt{-14}),$$

y es fácil ver que 3 es irreducible en $\mathbb{Z}[\sqrt{-14}]$. Veamos que $5 \pm 2\sqrt{-14}$ también lo son. Ambos tienen norma 81, por tanto si suponemos que $5 \pm 2\sqrt{-14} = ab$ entonces $N(a) \in \{1, 3, 9, 27, 81\}$. Si escribimos $a = x + y\sqrt{-14} \in \mathbb{Z}[\sqrt{-14}]$ tenemos

$$N(a) = x^2 + 14y^2$$

Claramente $N(a) \neq 3, 27$. Además, los únicos elementos en $\mathbb{Z}[\sqrt{-14}]$ con norma igual a 9 son ± 3, que no dividen a $5 \pm 2\sqrt{-14}$. Finalmente obtenemos que $N(a) = 1$ o $N(a) = 81$, es decir, a o b es unidad, por lo tanto $5 \pm 2\sqrt{-14}$ es irreducible.

Definición 7. Un anillo cuadrático $\mathbb{Z}[\alpha]$ se dice que es de norma Euclídea si para cada $A, B \in \mathbb{Z}[\alpha]$ con $B \neq 0$, existen $Q, R \in \mathbb{Z}[\alpha]$ tal que, $A = QB + R$ y $\big|N(R)\big| < \big|N(B)\big|$.

En particular, un anillo de norma Euclídea $\mathbb{Z}[\alpha]$ es un dominio Euclídeo, y por tanto sabemos que si $\mathbb{Z}[\alpha]$ es de norma Euclídea,entonces es un DIP y un DFU.

Ejemplo 5. Sea $\mathbb{Z}[i]$ el anillo de los enteros de Gauss, veamos que es de norma Euclídea.

Podemos cubrir el plano complejo por cuadrados de lado 1, centrando cada cuadrado en un entero de Gauss. Por el teorema de Pitágoras , la distancia del centro de uno de esos cuadrados a otro punto del cuadrado no es mayor que $\frac{1}{\sqrt{2}}$. Esto significa que para cada número complejo Z hay un entero de Gauss Q, tal que

$$\big|Q - Z\big| < \frac{1}{\sqrt{2}}$$

Veamos como se define el algoritmo de división.

Primero definimos el cociente Q como el entero de Gauss más cercano a $\frac{A}{B}$. Esto significa que Q es el centro del cuadrado que contiene al complejo $z = \frac{A}{B}$. Esto implica $\big|\frac{A}{B} - Q\big| \leq \frac{1}{\sqrt{2}}$ y tenemos que

$$\big|A - QB\big| \leq \frac{1}{\sqrt{2}}\big|B\big|$$

Por lo tanto $N(A - QB) \leq \frac{1}{2}N(B)$ y tomando como cociente Q, el resto debe ser $R = A - QB$. Tanto Q como R son enteros de Gauss, tenemos $A = QB + R$ y $N(R) \leq \frac{1}{2}N(B)$. Por lo tanto, $\mathbb{Z}[i]$ es de norma Euclídea.

Para ver como funciona en la práctica, sea $A = 34 + 6i$ y $B = 7 + 3i$. Tenemos

$$\frac{A}{B} = \frac{128}{29} - \frac{30}{29}i$$

El entero de Gauss más cercano a $\frac{A}{B}$ es $4 - i$, por lo cual tenemos $Q = 4 - i$ y $R = A - QB = 3 + i$. El resto R tiene norma 10 y $N(B) = 58$, por tanto $N(R) < N(B)$.

Lema 2. *Supongamos $Z \in \mathbb{Q}(\sqrt{d})$. Entonces existe $Q \in \mathbb{Z}[\alpha]$ tal que si $Z - Q = x + y\sqrt{d}$ se tiene que:*

1. $|x| \leq \frac{1}{2}$
2. *Si* $d \not\equiv 1$ *mod 4, entonces* $|y| \leq \frac{1}{2}$
3. *Si* $d \equiv 1$ *mod 4, entonces* $|y| \leq \frac{1}{4}$

Además, en los casos $d = -1, -2, -3, -7, -11, 2, 3, 5, 13$ *tenemos* $\left|N(Z-Q)\right| < 1$.

Demostración. Asumimos primero $d \not\equiv 1 \bmod 4$ y sea $Z = u + v\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ con $u, v \in \mathbb{Q}$.

En este caso, sea $Q = r + s\sqrt{d}$, con r y s los enteros más cercanos a u y v. En particular, $x = u - r$ e $y = v - s$ tienen valor absoluto $\leq \frac{1}{2}$.

En los casos $d = -1, -2$ tenemos:

$$0 \leq N(Z-Q) = x^2 - dy^2 \leq \frac{1+|d|}{4} < 1$$

En los casos $d = 2, 3$ la norma $x^2 - dy^2$ esta acotada por:

$$\frac{-3}{4} \leq -dy^2 \leq x^2 - dy^2 \leq x^2 \leq \frac{1}{4}$$

Por lo que $\left|N(Z-Q)\right| < 1$ en estos casos.

Asumiremos ahora que $d \equiv 1 \bmod 4$ y sea $Z = u + v\sqrt{d}$. Sea s el entero más cercano a $2v$, tendremos entonces que $|s - 2v| \leq \frac{1}{2}$. Esto implica $\left|\frac{s}{2} - v\right| \leq \frac{1}{4}$. Sea r el entero mas cercano a $u - \frac{s}{2}$. Tenemos que $\left|r + \frac{s}{2} - u\right| \leq \frac{1}{2}$. Si ponemos $Q = r + s\alpha$ entonces $Z - Q = x + y\sqrt{d}$ con $|x| = \left|u - r - \frac{s}{2}\right| \leq \frac{1}{2}$ e $|y| = \left|v - \frac{s}{2}\right| \leq \frac{1}{4}$.

Por lo tanto, en los casos $d = -3, -7, -11$ tenemos $0 \leq N(Z-Q) = x^2 - dy^2 \leq \frac{4+|d|}{16} < 1$.

En los casos reales cuadráticos $d = 5, 13$ tenemos

$$\frac{-13}{16} \leq -\frac{d}{16} \leq -dy^2 \leq x^2 - dy^2 \leq x^2 \leq \frac{1}{4}$$

En cada uno de los casos tenemos $\left|N(Z-Q)\right| < 1$.

□

Teorema 5. *Los anillos cuadráticos* $\mathbb{Z}[\alpha]$*, de* $\mathbb{Q}[\sqrt{d}]$ *con d=-1, -2, -3, -7, -11, 2, 3, 5 y 13 son de norma Euclídea.*

Demostración. Sea $A, B \in \mathbb{Z}[\alpha]$ con $B \neq 0$. Por el Lema anterior, podemos encontrar un $Q \in \mathbb{Z}[\alpha]$ tal que $\left|N(\frac{A}{B} - Q)\right| < 1$.

Sea $R = A - BQ$, entonces $A = QB + R$ y se tiene por tanto que
$\left|N(R)\right| = \left|N(A - BQ)\right| = \left|N(B)\right|\left|N(\frac{A}{B} - Q)\right| < N(R)$.

□

Nota 2. Se puede demostrar también que $\mathbb{Z}[\alpha]$ es de norma Euclídea en los casos

$$d = 6, 7, 11, 17, 19, 21, 29, 33, 37, 41, 57, 73$$

pero esto lleva un trabajo más complicado que en los casos anteriores. Vamos a ver un ejemplo de como usar el teorema anterior para aplicarlo a las ecuaciones diofánticas:

Ejemplo 6. Vamos a resolver la siguiente ecuación diofántica:

$$x^3 = y^2 + 11$$

Factorizando en $\mathbb{Q}(\sqrt{-11})$ tenemos $x^3 = (y + \sqrt{-11})(y - \sqrt{-11})$. El anillo de enteros de $\mathbb{Q}(\sqrt{-11})$ es el anillo cuadrático $\mathbb{Z}[\alpha]$, donde $\alpha = \frac{1+\sqrt{-11}}{2}$. Ya vimos que $\mathbb{Z}[\alpha]$ es de norma Euclídea y por tanto tiene factorización única. Veamos ahora que los factores $y + \sqrt{-11}$ e $y - \sqrt{-11}$ son coprimos. Sea D un factor común de ambos, y por lo tanto también de x. El elemento D será factor de $2\sqrt{-11}$ y por tanto de 22, si x fuese par tendríamos que $y^2 + 11 \equiv 0 \bmod 8$, que nos da una contradicción. Por lo tanto x es impar.

De manera similar, si x es múltiplo de 11 entonces $y^2 + 11 = 0 \bmod 11^3$ que da una contradicción. Como hemos visto que x es coprimo con 22, existirán enteros h y k tal que $22h + xk = 1$. Como D es un factor común de x y 22, D es un factor de 1 y por tanto una unidad.

Tenemos entonces $y + \sqrt{-11}$, $y - \sqrt{-11}$ son coprimos. Por el primer Lema, tenemos que $y + \sqrt{-11} = U(r + s\alpha)^3$ para algún $U \in \mathbb{Z}[\alpha]^x$ y $r, s \in \mathbb{Z}$. Por el primer teorema sabemos que $U = \pm 1$. Como -1 es un cubo, podíamos asumir sin perdida de generalidad que $U = 1$. Expandiendo la ecuación tenemos:

$$y - 1 + 2\alpha = r^3 + 3r^2 s\alpha + 3rs^2\alpha^2 + s^3\alpha^3$$

Como α es una raíz del polinomio $x^3 - x + 3$, tenemos $\alpha^2 = \alpha - 3$. Esto implica $\alpha^2 = -2\alpha - 3$, y por lo tanto

$$y - 1 + 2\alpha = (r^3 - 9rs^2 - 3s^2) + (3r^2 s + 3rs^2 - 2s^3)\alpha$$

Comprobando los coeficientes de 1 y α, tenemos las ecuaciones:

$$y - 1 = r^3 - 9rs^2 - 3s^2 \qquad y \qquad 3r^2 s + 3rs^2 - 2s^3 = 2$$

La segunda ecuación muestra que s es un factor de 2, por tanto $s = \pm 1, \pm 2$.

Vamos a considerar cada caso. Si $s = 1$, entonces la segunda ecuación se reduce a $3r^2 + 3r - 2 = 0$ que no tiene soluciones enteras. Si $s = -1$ tenemos que $-3r^2 + 3r + 2 = 2$ que tiene solución $r = 0$, $r = 1$. Sustituyendo en la primera tenemos que $y = \pm 4$, que nos da las soluciones (3,4) y (3,-4) de la ecuación diofántica.

En el caso $s = 2$, tenemos $6r^2 + 12r - 16 = 2$. Esta tiene soluciones $r = 1$, $r = -3$ que nos da $y = \pm 58$. Obtenemos entonces (15,58) y (15,-58).

Finalmente en el caso $s = -2$, tenemos $-6r^2 + 12r + 16 = 2$, que no tiene soluciones enteras. Por lo tanto hemos visto que la ecuación $x^3 = y^2 + 11$ tiene cuatro soluciones enteras que son

$$(3, 4), (3, -4), (15, 58), (15, -58)$$

Nota 3. (Otros anillos de factorización única)

El Teorema 5 nos da varios ejemplos de anillos cuadráticos de norma Euclídea. Por tanto estos anillos tienen factorización única. Hay también ejemplos de anillos cuadráticos con factorización única que no son de norma Euclídea. Se sabe que un anillo cuadrático complejo tiene factorización única para los siguientes valores de d y no más:

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163$$

Este resultado fue conjeturado por Gauss. Hay dos demostraciones, una realizada por Baker y otra por Stark([7], [8]). Es relativamente fácil demostrar que estos anillos $\mathbb{Z}[\alpha]$ tienen factorización única, lo difícil es ver que los demás no la tienen.

El primero que no esta en esta lista es $\mathbb{Z}[\sqrt{-5}]$, es fácil ver que no es de factorización única. Por ejemplo:

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

Es fácil ver que los elementos 2,3 y $1 \pm \sqrt{-5}$ son todos irreducibles en $\mathbb{Z}[\sqrt{-5}]$. Por tanto son dos descomposiciones distintas de 6 y $\mathbb{Z}[\sqrt{-5}]$ no es DFU. En contraste, es más común para un anillo cuadrático real tener factorización única. Existe una conjetura que dice que hay infinitos anillos reales cuadráticos con factorización única.

Por ejemplo, $\mathbb{Z}[\alpha]$ tiene factorización única para los siguientes valores de d:

$$d = 2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29, 31, 33, 37 \ .$$

1.5. Descomposición de primos en anillos cuadráticos

En esta sección caracterizaremos los elementos irreducibles de un anillo cuadrático.

Lema 3. *Sea $\mathbb{Z}[\alpha]$ un anillo cuadrático con factorización única. Si Q es un elemento irreducible de $\mathbb{Z}[\alpha]$, entonces hay un único primo p en $\mathbb{Z}$, tal que Q es un factor de p.*

Demostración. (Existencia) El elemento Q divide algún entero n, por ejemplo divide a su norma $N(Q) = Q\overline{Q}$. Por otro lado, si $n = ab$, entonces por la factorización única, Q es un factor de a o b. Por lo tanto, si factorizamos n en primos de $\mathbb{Z}$, entonces uno de esos primos es un múltiplo de Q.

(Unicidad) Supongamos que Q es un factor de dos primos distintos p y q. Por el Lema de Bezout, podemos encontrar enteros h y k tal que $1 = hp + kq$. Por tanto, Q es un factor de 1, y por tanto es una unidad. Esto es una contradicción ya que los elementos irreducibles no son unidades.

□

Observación 3. El Lema muestra que para describir los elementos irreducibles en $\mathbb{Z}[\alpha]$, nosotros necesitamos factorizar los primos de $\mathbb{Z}$ en el anillo $\mathbb{Z}[\alpha]$. Veamos ahora las maneras en las que se puede factorizar un primo p. Si $Q_1 \in \mathbb{Z}[\alpha]$ es un factor irreducible de un número primo p, entonces $N(Q_1)$ debe ser un factor de $N(p)$. Como $N(P) = p^2$, esto implica que $N(Q_1)$ es o bien $\pm p$ o $\pm p^2$. En el caso $N(Q_1) = \pm p^2$, debemos tener que $p = UQ_1$ para una unidad U, y por lo tanto p es el mismo irreducible en $\mathbb{Z}[\alpha]$. En este caso, decimos que p es **inerte** en $\mathbb{Z}[\alpha]$.

En el caso que Q_1 tiene norma $\pm p$, tenemos $p = Q_1Q_2$, donde Q_2 tiene norma $\pm p$. En este caso, p no es irreducible en $\mathbb{Z}[\alpha]$. De hecho ya que $Q_1\overline{Q_1} = N(Q_1) = \pm p$, esto nos da que $Q_2 = \pm\overline{Q_1}$, y Q_2 es también irreducible.

Distinguiremos entre dos casos diferentes: si $Q_2 = UQ_1$ con U unidad tendremos que $p = UQ_1^2$ y diremos que p es **ramificado**. En otro caso $\frac{Q_1}{Q_2} \notin \mathbb{Z}[\alpha]$ y $p = Q_1Q_2$ con Q_1 y Q_2 no asociados. En esta caso diremos que p es **divisible** en $\mathbb{Z}[\alpha]$.

Como resumen el primo p es inerte, ramificado o divisible, dependiendo de los siguientes casos:

1. p es irreducible en $\mathbb{Z}[\alpha]$
2. $p = UQ^2$, donde U es una unidad y Q es irreducible con norma $\pm p$.
3. $p = Q_1Q_2$, donde Q_1 y Q_2 son elementos irreducibles con norma $\pm p$ y Q_1, Q_2 no son asociados.

Ejemplo 7. Considerando el anillo $\mathbb{Z}[i]$ de los enteros de Gauss. Un primo p se factorizará en el anillo si hay elementos con norma p. Si nosotros tenemos un elemento Q con norma p, entonces la factorización es $p = Q\overline{Q}$. Notese que $N(x+iy) = x^2+y^2$, así que para ver que p factoriza tenemos que calcular las soluciones enteras de la ecuación $x^2 + y^2 = p$. Algún ejemplo será:

1. $2 = 1^2 + 1^2 = (1 + i)(1 - i) = -i(1 + i)^2$ por tanto 2 es ramificado
2. $5 = 2^2 + 1^2 = (2 + i)(2 - i)$ entonces 5 es divisible
3. $13 = 3^2 + 2^2 = (3 + 2i)(3 - 2i)$, y 13 es divisible

$3, 7, 11$ son inertes en $\mathbb{Z}[i]$, ya que no podemos escribirlos en la forma $x^2 + y^2$

El siguiente teorema nos dice exactamente que primos son inertes, ramificados y divisibles, pero antes daremos una definición del símbolo de Legendre:

Definición 8. Sea p un primo impar y $a \in \mathbb{Z}$. El símbolo de Legendre $\left(\frac{a}{p}\right)$ se define de la siguiente manera:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } p \text{ divide a } a \\ 1 & \text{si existe } x \in \mathbb{Z} \text{ tal que } x^2 \equiv a \text{ (mod p) y } p \text{ no divide a } a \\ -1 & \text{en otro caso} \end{cases} \tag{1.4}$$

Es decir, si $p \not| a$, tendremos que $\left(\frac{a}{p}\right) = 1$ si a es un residuo cuadrático módulo p y $\left(\frac{a}{p}\right) = -1$ si no es a un residuo cuadrático módulo p.

Teorema 6. *Sea $\mathbb{Z}[\alpha]$ el anillo cuadrático de $\mathbb{Q}[\sqrt{d}]$. Supongamos que $\mathbb{Z}[\alpha]$ tiene factorización única y sea p un primo impar, entonces:*

1. *p es ramificado si y solo si p es un factor de d.*
2. *p es divisible si y solo si $\left(\frac{d}{p}\right) = 1$.*

3. p es inerte si y solo si $\left(\frac{d}{p}\right) = -1$.

Además , para el número primo 2 se tiene que es divisible si $d \equiv 1$ mod 8, es inerte si $d \not\equiv 5$ mod 8 y es ramificado en los otros casos.

Demostración. Más que ver los casos especiales, asumiremos por simplicidad que $d \not\equiv 1 \bmod 4$ por lo que el anillo cuadrático es $\mathbb{Z}[\sqrt{d}]$, y la norma dada es $N(x + y\sqrt{d}) = x^2 - dy^2$. Los otros casos son similares.

(1)Supongamos primero que p es un factor de d, par o impar. Vamos a ver que es ramificado. Sea Q un factor irreducible de p. Para ver que p es ramificado es suficiente con ver que Q^2 es un factor de p.

Nótese que Q es un factor de $d = (\sqrt{d})^2$. Como Q es irreducible, Q debe ser un factor de $\sqrt{d}$, y por lo tanto Q^2 es un factor de d. Como d es libre de cuadrados, el mayor factor común de d y p^2 es p, por lo que podemos encontrar enteros h, k tal que $p = hd + kp^2$. Ya que Q^2 es un factor común de d y p^2, se tiene que Q^2 es un factor de p, por lo que p es ramificado.

(2)Ahora consideramos el primo $p = 2$ en los casos que d es impar. Como estamos asumiendo que $d \not\equiv 1 \bmod 4$, intentaremos ver que 2 es ramificado. Sea Q un factor irreducible de 2 en $\mathbb{Z}[\alpha]$, otra vez veremos que Q^2 es un factor de 2.

Notese que $(1+\sqrt{d})^2 = 1+d+2\sqrt{d}$, que es múltiplo de 2. Esto muestra que Q es un factor de $(1 + \sqrt{d})^2$, y por tanto de $1 + \sqrt{d}$. De la misma forma, sabemos que Q es un factor de $1+\sqrt{d}$. Por lo tanto Q^2 es un factor de $(1+\sqrt{d})(1-\sqrt{d}) = 1-d$. Ya que $m.c.d(1-d, 4) = 2$, podemos encontrar enteros h y k tal que $4h + (1-d)k = 2$.

Ya que Q^2 es un factor común de 4 y $1 - d$, esto sigue que Q^2 es un factor de 2, por lo que 2 es ramificado.

(3)Hasta aquí, hemos visto que si p es un factor de $2d$, entonces p es ramificado. A la inversa, asumiremos que p es ramificado, entonces hay un elemento $Q = x + y\sqrt{d}$ tal que Q^2 es un múltiplo de p, pero Q no es un múltiplo de p. Como $Q^2 = (x^2 + dy^2) + 2xy\sqrt{d}$ sabemos que:

$$x^2 + dy^2 \equiv 0 \quad \text{mód } p \qquad\qquad 2xy \equiv 0 \quad \text{mód } p$$

pero x e y no son ambos múltiplos de p. De hecho, y no es múltiplo de p, ya que por otra parte, la primera ecuación forzará que x sea también múltiplo de p. Como y es invertible módulo p, la segunda ecuación implica $2x \equiv 0 \bmod p$. Por la primera ecuación, tenemos $4dy^2 \equiv 0 \bmod p$. Ya que y es invertible, esto sigue que $4d \equiv 0 \bmod p$, por tanto p es un factor de $2d$.

(4)Ahora debemos asumir que p no es un factor de $2d$, por lo que p es inerte o divisible. Supongamos que p es divisible, por tanto hay un elemento $Q = x + y\sqrt{d}$ con norma $\pm p$. Entonces tenemos $x^2 - dy^2 = \pm p$.

Supongamos p un factor de y. Entonces tenemos que $x^2 \equiv \pm p \bmod p^2$. Esto implica que p es un factor de x, y por lo tanto $0 = \pm p \bmod p^2$, que nos da una contradicción. De esto deducimos que y es invertible módulo p, y por tanto $\left(\frac{x}{y}\right) \equiv d \bmod p$. En particular, d es un residuo cuadrático módulo p.

(5)De manera inversa, supongamos $x_2 \equiv d \bmod p$ y sea $A = x + \sqrt{d}$. Claramente p es un factor de $x^2 - d = A\overline{A}$, pero p no es un factor de A ni $\overline{A}$. Por lo tanto, p no es irreducible por lo que es divisible.

□

Nota 4. En el caso en que el anillo de enteros cuadráticos $\mathbb{Z}[\alpha]$ es un DFU, el Teorema anterior permite describir el conjunto de sus elementos irreducibles. Este hecho, junto con la descripción de la unidades el anillo, nos proporciona la factorización de cualquier elemento del anillo y por tanto permite describir el anillo en base a sus unidades y su conjunto de irreducibles. Para completar la descripción, a la vista de los resultados ya probados sobre las unidades del anillo, nos falta calcular el grupo de unidades o, más concretamente, la unidad fundamental. Para ello desarrollaremos la teoría de fracciones continuas en el capítulo siguiente.

Un criterio para la factorización única

Resulta que uno también puede mostrar que un anillo tiene factorización única solo comprobando las predicciones del Teorema de Descomposición. Para aclarar esto, notese que dicho teorema nos dice que números primos factorizan en $\mathbb{Z}[\alpha]$. Sea:

$$S_d = \{\text{primos } p : \ p|d \ o \left(\frac{d}{p}\right) = 1 \ o \ (p = 2 \ y \ d \not\equiv 5 \ mod \ 8)\}.$$

El Teorema de Descomposición nos dice que si $\mathbb{Z}[\alpha]$ tiene factorización única, entonces para cada primo $p \in S_d$, hay un elemento con norma $\pm p$. El recíproco también cierto, y nos da una manera de probar que $\mathbb{Z}[\alpha]$ tiene factorización única, incluso en el caso donde el anillo no es de norma Euclídea. Por supuesto, el conjunto S_d es infinito, es un método inabordable en la práctica.

Pero se puede decir más, uno solo necesita comprobar una cantidad finita de primos en S_d. Con más precisión, definimos el número real positivo M_d como sigue:

$$M_d = \begin{cases} \sqrt{|d|} & \text{si } d > 0 \text{ y } d \equiv 1 \bmod 4 \\ 2\sqrt{|d|} & \text{si } d > 0 \text{ y } d \not\equiv 1 \bmod 4 \\ \frac{2}{\pi}\sqrt{|d|} & \text{si } d < 0 \text{ y } d \equiv 1 \bmod 4 \\ \frac{4}{\pi}\sqrt{|d|} & \text{si } d < 0 \text{ y } d \not\equiv 1 \bmod 8 \end{cases} \tag{1.5}$$

El número M_d se llama número de Minkowski, y se tiene:

Teorema 7. *Sea $\mathbb{Z}[\alpha]$ un anillo cuadrático y sea M_d el correspondiente número de Minkowski. Entonces $\mathbb{Z}[\alpha]$ tiene factorización única si y solo si para cada número primo p con $p < M_d$ hay un elemento de $\mathbb{Z}[\alpha]$ con norma $\pm p$.*

La prueba de este teorema se basa en el concepto de ideal, y queda fuera del contexto de este trabajo. Se puede probar usando resultados de teoría de números algebraicos como ([9]).

Ejemplo 8. Veamos que el anillo $\mathbb{Z}\Big[\frac{1+\sqrt{-163}}{2}\Big]$ tiene factorización única. El límite de Minkowski en este caso es

$$M_{-163} = \frac{2\sqrt{163}}{\pi} \approx 25{,}534$$

Los primos menores que el límite son:

$$2, 3, 5, 7, 11, 13, 17, 19, 23$$

Como $-163 \equiv 5 \bmod 8$, el primo 2 no esa en S_{-163}. El número 163 es primo, así que ninguno de los primos de la lista es factor de 163. Más aún, podemos comprobar $\left(\frac{-163}{p}\right) = -1$ para cada primo impar de la lista.

Por lo tanto, no hay primos menores que el límite de Minkowski en S_{-163} y por el teorema anterior, el anillo tiene factorización única.

Notese que

$$N(x + \alpha) = x^2 + x + 41$$

El polinomio $m(x) = x^2 + x + 41$ es conocido porque los números $m(0), m(1), \ldots, m(39)$ son primos. Veremos el corolario siguiente:

Corolario 2. *Para $x = 0, 1, \ldots, 39$ el número $x^2 + x + 41$ es primo.*

Demostración. Sea x un entero entre 0 y 39. Supongamos x^2+x+41 es compuesto, y sea p el primo más pequeño. Entonces tenemos $p^2 \leq x^2 + x + 41$ y esto implica $p < 40$. Si tomamos $\alpha = \dfrac{1 + \sqrt{-163}}{2}$, entonces ningún número algebraico $x + \alpha$ ni $x + \overline{\alpha}$ es múltiplo de p en $\mathbb{Z}[\alpha]$, mientras que su producto, que es $m(x)$ es múltiplo de p en $\mathbb{Z}$ y $\mathbb{Z}[\alpha]$.

Como $\mathbb{Z}[\alpha]$ tiene factorización única, esto nos dice que p no es irreducible en $\mathbb{Z}[\alpha]$, por lo que debe haber algún elemento $r + s\alpha$ con norma p. En particular, tenemos $r^2 + rs + 41s^2 = p$. Completando cuadrados, vemos que $40s^2 \leq p < 40$ y por tanto $s = 0$. Esto implica $r^2 = p$ que nos da una contradicción ya que p es primo.

□

Ecuaciones diofánticas para la norma $N(A) = n$

Vamos a resolver la pregunta de cuántos enteros se pueden escribir como $|N(A)|$ para algún $A \in \mathbb{Z}[\alpha]$. Nos restringiremos a los casos en que $\mathbb{Z}[\alpha]$ tiene factorización única.

Ejemplo 9. Sea $d = -1$, tendremos el anillo cuadrático $\mathbb{Z}[i]$ de los enteros de Gauss. Entonces $N(x + iy) = x^2 + y^2$. Veamos qué enteros tienen la forma $x^2 + y^2$ con $x, y \in \mathbb{Z}$. Algún ejemplo será:

$$2 = 1^2 + 1^2, 4 = 2^2 + 0^2, 5 = 2^2 + 1^2, 8 = 2^2 + 2^2, 9 = 3^2 + 0^2$$

Por lo tanto los número 3,6 y 7 no se pueden escribir como suma de cuadrados.

La respuesta se sigue facilmente por el Teorema de Descomposición. En general, un elemento $A \in \mathbb{Z}[\alpha]$ es un producto de elementos irreducibles. Por lo tanto, la norma de A es un producto de normas de elementos irreducibles. Si p es ramificado o divisible, entonces hay un elemento irreducible de norma $\pm p$. Si p es inerte, entonces es irreducible y su norma es p^2. Por lo tanto, la potencia de cada primo inerte en $N(A)$ tiene que ser par.

Definición 9. Sea p un número primo, diremos que $\nu_p(n)$ es el mayor entero a tal que p^a es un factor de n.

Corolario 3. *Sea $\mathbb{Z}[\alpha]$ un anillo cuadrático con factorización única. Sea n un entero positivo. Son equivalentes:*

1. *Existe un elemento $A \in \mathbb{Z}[\alpha]$ tal que $|N(A)| = n$*
2. *Para cada primo p que divide a n , si p es inerte en $\mathbb{Z}[\alpha]$, entonces $\nu_p(n)$ es par.*

Demostración. Supondremos que $|N(A)| = n$ y factorizamos A en elementos irreducibles $A = Q_1 \dots Q_n$.

Entonces $|N(Q_i)|$ es o bien un número primo p_i o p_i^2 si p_i es inerte. Por lo tanto, si $D = \{p_i : \quad p_i \text{ primo inerte}\}$,y $E = \{p_i : \quad p_i \text{ primo ramificado o divisible}\}$:

$$|N(A)| = \prod_{p_i \in D} p_i^2 \prod_{p_i \in E} p^i \ .$$

En particular, las potencias de los primos inertes son pares.

Recíprocamente, supongamos

$$n = \prod_{p_i \in D} p_i^{2r_i} \prod_{p_i \in E} p_i^{r_i} \ .$$

Eligiendo elementos irreducibles Q_i tal que $|N(Q_i)| = p_i$ o p_i^2. Si definimos $A = \prod Q_i^{r_i}$, entonces claramente $|N(A)| = n$.

□

Ejemplo 10. Escribiremos 585 como suma de dos cuadrados en todos las maneras posibles. Es lo mismo que encontrar todos los enteros de Gauss de norma 585.

$$585 = 3^2 \cdot 5 \cdot 13$$

El primo 3 es inerte en $\mathbb{Z}[i]$, esto significa que 3 es irreducible y tiene norma 3^2. los primos 5 y 13 son divisibles, con factores de norma 5 y 13.

$$5 = (2+i)(2-i) \qquad 13 = (3+2i)(3-2i)$$

Esto significa que cada elemento de norma 5 es una unidad múltiplo de $2+i$ o $2-i$ y cada elemento de norma 13 es una unidad múltiplo de $3+2i$ o $3-2i$. Por lo tanto, los elementos de norma 585 son unidades múltiplos de cada uno de los siguientes elementos.

$$3(2+i)(3+2i) = 12+21i$$

$$3(2+i)(3-2i) = 24-3i$$
$$3(2-i)(3+2i) = 24+3i$$
$$3(2-i)(3-2i) = 12-21i$$

Como $\mathbb{Z}[i]$ tiene cuatro unidades, hay 16 soluciones a la ecuación $x^2+y^2 = 585$. Por lo tanto, muchas de estas soluciones se parecen. Asumimos que x e y son ambos positivos y $x \leq y$, entonces tenemos las dos soluciones

$$585 = 12^2 + 21^2 = 3^2 + 24^2$$

Las otras soluciones se obtienen cambiando signos o cambiando x por y.

Ejemplo 11. Consideramos la ecuación $x^2+xy+y^2 = 150$. Notese que $x^2+xy+y^2 = N(x+y\alpha)$ en el caso $d = -3$ (enteros de Eisenstein). El número 150 factoriza $2*3*5^2$. Por el Teorema de Descomposición, 2 es inerte, 3 es ramificado y 5 es inerte. Como $\nu_2(150) = 1$, que es impar, la ecuación no tiene solución.

Ejemplo 12. Resolveremos la ecuación $x^2+xy+y^2 = 84$, $84 = 2^2 \cdot 3 \cdot 7$. Tenemos $\left(\frac{-3}{7}\right) = 1$ Por el Teorema de Descomposición 2 es inerte, 3 ramificado y 7 divisible. Los factores de 3 y 7 son:

$$3 = -\sqrt{-3}^2 = -(2\alpha-1)^2 \qquad \text{y} \qquad 7 = N(2+\alpha) = (2+\alpha)(3-\alpha)$$

Los enteros de Eisenstein de norma 84 son unidades múltiplos o bien de $2(2\alpha-1)(2+\alpha)$ o bien de $2(2\alpha-1)(3-\alpha)$. Usando el hecho de que $\alpha^2+\alpha+1 = 0$ encontramos que esos dos números son $10\alpha-8$ y $2-10\alpha$. Hay seis unidades en los enteros de Eisenstein, así que en total 12 elementos de norma 84. Por ejemplo:

$$84 = N(10\alpha-8) = 10^2 + 10(-8) + (-8)^2$$

.

Capítulo 2

Fracciones continuas

Las fracciones continuas son un mecanismo útil en aritmética y teoría de números para aproximar por números racionales y de manera eficiente los números irracionales. Su uso se extiende a muchos más problemas, por ejemplo en la resolución de ecuaciones diofánticas o en problemas de factorización de enteros. En nuestro contexto, además del interés por sí mismas, son un ingrediente básico en el cálculo eficiente de las unidades de los anillos de números cuadráticos reales. El concepto de fracción continua se puede entender fácilmente con conocimientos de aritmética.

2.1. Introducción y primeros resultados

Veamos un ejemplo desarrollando la fracción $\frac{91}{43}$:

$$\frac{91}{43} = 2 + \frac{5}{43} = 2 + \frac{1}{\frac{43}{5}} = 2 + \frac{1}{8 + \frac{3}{5}} = 2 + \frac{1}{8 + \frac{1}{1+\frac{1}{3}}} \, .$$

Una fracción continua continua finita es una expresión del tipo

$$z_1 + \cfrac{b_1}{z_2 + \cfrac{b_2}{z_3 + \cfrac{b_3}{\ddots + \cfrac{b_{n-1}}{z_{n-1} + \cfrac{b_n}{z_n}}}}}$$

donde z_i, $b_i \in \mathbb{C}$ con $i = 1, \ldots, n$. Evidentemente la expresión anterior, siempre que los sucesivos denominadores sean no nulos, define un número complejo x.Nosotros usaremos una versión menos general. Llamaremos *fracción continua finita* a una expresión del tipo

$$[z_1, z_2, \ldots, z_n] = z_1 + \cfrac{1}{z_2 + \cfrac{1}{\ddots + \cfrac{1}{z_{n-1} + \cfrac{1}{z_n}}}}$$

donde $z_1, \ldots, z_n \in \mathbb{R}$ y $z_2, \ldots, z_n > 0$.

En nuestro ejemplo tenemos:

$$\frac{91}{43} = [2, 8, 1, 3] \, .$$

A lo largo de la historia ha habido matemáticos que usaban otras notaciones,por ejemplo, Pietro Antonio Cataldi (1548-1626) usaba la notación : $z_1 \cdot \&\frac{b_1}{z_2.} \cdot \&\frac{b_2}{z_3.}$, y Maritz Abraham Stern(1807-1894) usaba: $z_1 + \frac{b_1|}{|z_2.} + \frac{b_2|}{|z_3.} + \ldots$

Observación 4. Antes de empezar con definiciones precisas y resultados vamos a ver como se relacionan las fracciones continuas con el **algoritmo de Euclides** :

Sean dos números enteros r_0, r_1 con $r_1 > 0$. Entonces la división euclídea nos proporciona sucesivamente números enteros $y_1, \ldots, y_n, r_2, \ldots, r_n$ con:

$$\begin{aligned} r_0 &= y_1 r_1 + r_2 && 0 < r_2 < r_1 \\ r_1 &= y_2 r_2 + r_3 && 0 < r_3 < r_2 \\ &\ldots \\ r_{n-2} &= y_{n-1} r_{n-1} + r_n && 0 < r_n < r_{n-1} \\ r_{n-1} &= y_n r_n \end{aligned}$$

Ahora ponemos: $x = \frac{r_0}{r_1} = y_1 + \frac{r_2}{r_1} = y_1 + \frac{1}{r_1/r_2}$. Notese además que $\frac{r_1}{r_2} > 1$. Ahora $\frac{r_1}{r_2} = y_2 + \frac{r_3}{r_2}$ y por tanto

$$\frac{r_0}{r_1} = y_1 + \frac{1}{y_2 + \frac{r_3}{r_2}} = y_1 + \frac{1}{y_2 + \frac{1}{r_2/r_3}} \, .$$

Continuando el proceso llegamos a que el número racional $x = \frac{r_0}{r_1}$ se escribe como $x = [y_1, y_2, \ldots, y_n]$ y la fracción continua en este caso expresa el número racional x en función de los cocientes sucesivos que proporciona el algoritmo de Euclides.

Observese también que $y_1 = \lfloor \frac{r_0}{r_1} \rfloor = \lfloor x \rfloor$ y $x - y_1 = x - \lfloor x \rfloor$, siendo $\lfloor x \rfloor$ el mayor entero menor o igual que x, es decir, su parte entera por defecto. Por tanto tenemos que $\frac{r_1}{r_2} = \frac{1}{x - \lfloor x \rfloor}$.

Siguiendo esta idea, la construcción anterior se puede extender a un número real cualquiera. Es decir, sea $x \in \mathbb{R}$. Podemos definir $y_1 = \lfloor x \rfloor \in \mathbb{Z}$, si $x \neq \lfloor x \rfloor$, $x_1 = \frac{1}{x - \lfloor x \rfloor} > 1$ y tenemos que $x = y_1 + \frac{1}{x_1}$. Repitiendo el proceso para x_1 podemos construir directamente $y_2, \ldots, y_n \in \mathbb{Z}_+$ y $x_n \in \mathbb{R}$, $x_n > 1$ de manera que podemos expresar x como la fracción continua

$$x = [y_1, y_2, \ldots, y_n, x_n].$$

Nota 5. Obsérvese que si $x = \frac{r_0}{r_1} \in \mathbb{Q}$, $r_0, r_1 \in \mathbb{Z}$ y $x = [y_1, \ldots, y_n]$ entonces $y_1, \ldots, y_n \in \mathbb{Z}$ y además $y_2, \ldots, y_n \geq 1$. Si tenemos $x \in \mathbb{R}$ tenemos $x = [y_1, \ldots, y_n, x_n]$ con $y_2, \ldots, y_n \in \mathbb{Z}$, $x_n \in \mathbb{R}$ y además $y_2, \ldots, y_n, x_n \geq 1$.

Definición 10. Dada una fracción continua finita $[z_1, \ldots, z_n]$, al número real $c_i = [z_1, \ldots, z_i]$ $(i = 1, 2, \ldots, n)$ se le llama i-ésimo convergente.

Observemos que $c_1 = \frac{z_1}{1} = \frac{p_1}{q_1}$ donde $p_1 = z_1$ y $q_1 = 1$. Para c_2 tenemos $c_2 = z_1 + \frac{1}{z_2} = \frac{z_1 z_2 + 1}{z_2} = \frac{p_2}{q_2}$ donde $p_2 = z_1 z_2 + 1$ y $q_2 = z_2$. De la misma forma

$$c_3 = [z_1, z_2, z_3] = \frac{z_1 z_2 z_3 + z_1 + z_3}{z_2 z_3 + 1} = \frac{p_3}{q_3}$$

con $p_3 = z_3 p_2 + p_1$ y $q_3 = z_3 q_2 + q_1$ y podemos continuar el proceso.

Definición 11. Dada la fracción continua finita $[z_1 \ldots, z_n]$, definamos $p_0 = 1$, $q_0 = 0$, $p_{-1} = 0$, $q_{-1} = 1$ y para $i \geq 1$:

$$p_i = z_i p_{i-1} + p_{i-2} \qquad\qquad q_i = z_i q_{i-1} + q_{i-2} \ .$$

Proposición 5. *Sea $[z_1, z_2, \ldots, z_n]$ una fracción continua finita, para $i = 1, \ldots, n$ se tiene que*

$$c_i = [z_1, \ldots, z_n] = \frac{p_i}{q_i} \ .$$

Demostración. Razonamos por inducción sobre la longitud, n, de la fracción continua. Para una fracción de longitud $1, 2$ y 3, ya conocemos que es válida. Sea ahora una fracción continua $[z_1, \ldots, z_n]$ de longitud n y supongamos que la fórmula es válida para toda fracción continua $[y_1, \ldots, y_k]$ de longitud $k < n$.

Ahora, si $i < n$, tenemos $c_i = [z_1, \ldots, z_n] = \frac{p_i}{q_i}$ por hipótesis de inducción. Por lo tanto solo hay que demostrar el caso $i = n$. Observemos que

$$c_n = [z_1, \ldots, z_n] = [z_1, \ldots, z_{n-2}, y_{n-1}]$$

siendo $y_{n-1} = z_{n-1} + \frac{1}{z_n}$. Puesto que la longitud de $[z_1, \ldots, z_{n-2}, y_{n-1}]$ es $n-1$ y su $(n-1)$-ésimo convergente es $\frac{p'_{n-1}}{q'_{n-1}}$ con

$$p'_{n-1} = y_{n-1} p_{n-2} + p_{n-3} \quad q'_{n-1} = y_{n-1} q_{n-2} + q_{n-3}$$

tendremos:

$$\begin{aligned} c_n = \frac{p'_{n-1}}{q'_{n-1}} &= \frac{\left(z_{n-1} + \frac{1}{z_n}\right) p_{n-2} + p_{n-3}}{\left(z_{n-1} + \frac{1}{z_n}\right) q_{n-2} + q_{n-3}} \\ &= \frac{(z_n z_{n-1} + 1) p_{n-2} + p_{n-3} z_n}{(z_n z_{n-1} + 1) q_{n-2} + q_{n-3} z_n} \\ &= \frac{z_n (z_{n-1} p_{n-2} + p_{n-3}) + q_{n-2}}{z_n (z_{n-1} q_{n-2} + q_{n-3}) + q_{n-2}} \\ &= \frac{z_n p_{n-1} + p_{n-2}}{z_n q_{n-1} + q_{n-2}} = \frac{p_n}{q_n}. \end{aligned}$$

□

Proposición 6. *Sea $[z_1, z_2, \ldots, z_n]$ una fracción continua finita, entonces*

$$p_i q_{i-1} - p_{i-1} q_i = (-1)^i \qquad\qquad \text{para todo } i = 1, \ldots, n$$

Demostración. Tenemos que cuando $i = 1$, $p_1 q_0 - p_0 q_1 = z_1 \cdot 0 - 1 \cdot 1 = (-1)^1$ con $i = 2$ se tiene que $p_2 q_1 - p_1 q_2 = (z_2 z_1 + 1) \cdot 1 - z_1 z_2 = 1 = (-1)^2$.

Como en la proposición anterior razonamos por inducción y vamos por tanto a suponer que se cumple para un cierto i, veremos a ver si se cumple para $i + 1$. Por la proposición anterior tenemos que para $i + 1$

$$p_{i+1} = z_{i+1} p_i + p_{i-1} \qquad \text{y} \qquad q_{i+1} = z_{i+1} q_i + q_{i-1}$$

por lo tanto podemos escribir

$$\begin{aligned} p_{i+1}q_i - p_iq_{i+1} &= (z_{i+1}p_i + p_{i-1})q_i - p_i(z_{i+1}q_i + q_{i-1}) \\ &= z_{i+1}p_iq_i + p_{i-1}q_i - z_{i+1}p_iq_i - p_iq_{i-1} \\ &= (-1)(p_iq_{i-1} - p_{i-1}q_i) \end{aligned}$$

Esto basta para concluir ya que hemos supuesto que es cierto para i, y por tanto $p_iq_{i-1} - p_{i-1}q_i = (-1)^i$, con lo que sustituyendo en la igualdad anterior llegamos a

$$p_{i+1}q_i - p_iq_{i+1} = (-1)(-1)^i = (-1)^{i+1}.$$

□

Proposición 7. *Sea $c_i = \frac{p_i}{q_i}$ el i-ésimo convergente de la fracción continua $[z_1, z_2, \ldots, z_i]$. Entonces se tiene que*

$$c_i - c_{i-1} = \frac{(-1)^i}{q_{i-1}q_i} \qquad c_i - c_{i-2} = \frac{z_i(-1)^{i-1}}{q_iq_{i-1}}.$$

Como consecuencia, el valor absoluto de la diferencia entre dos convergentes consecutivos, c_i y c_{i-1}, es $|c_i - c_{i-1}| = \frac{1}{q_{i-1}q_i}$.

Demostración. Sabemos que $p_iq_{i-1} - p_{i-1}q_i = (-1)^i$. Al dividir entre $q_{i-1}q_i$ en ambos lados de la igualdad se tiene que

$$\frac{p_i}{q_i} - \frac{p_{i-1}}{q_{i-1}} = \frac{(-1)^i}{q_{i-1}q_i} \quad \text{es decir, } c_i - c_{i-1} = \frac{(-1)^i}{q_iq_{i-1}}$$

y queda demostrada la primera igualdad. Veamos ahora la segunda igualdad, primero tenemos que

$$c_i - c_{i-2} = \frac{p_i}{q_i} - \frac{p_{i-2}}{q_{i-2}} = \frac{p_iq_{i-2} - p_{i-2}q_i}{q_iq_{i-2}}.$$

Sabemos que $p_i = z_ip_{i-1} + p_{i-2}$ y $q_i = z_iq_{i-1} + q_{i-2}$. Obtenemos por tanto

$$\begin{aligned} p_iq_{i-2} - p_{i-2}q_i &= (z_ip_{i-1} + p_{i-2})q_{i-2} - p_{i-2}(z_iq_{i-1} + q_{i-2}) \\ &= z_i(p_{i-1}q_{i-2} - p_{i-2}q_{i-1}) \\ &= z_i(-1)^{i-1}. \end{aligned}$$

□

2.2. Fracciones continuas simples finitas

Definición 12. Llamaremos fracción continua simple finita a una expresión de la forma $[a_1, a_2, \ldots, a_n]$ donde a_1 es un entero positivo o negativo, y los términos $a_2, \ldots, a_n$ son enteros positivos. Llamaremos a $a_1, \ldots, a_n$ los cocientes parciales de la fracción continua.

Evidentemente una fracción continua simple finita define un número racional. Veamos como sería $[1,2,3,2]$

$$[1,2,3,2] = 1 + \frac{1}{2 + \frac{1}{3+\frac{1}{2}}} = 1 + \frac{1}{2+\frac{2}{7}} = 1 + \frac{7}{16} = \frac{23}{16}$$

Ahora veamos $\frac{67}{29}$ y $\frac{29}{67}$

$$\frac{67}{29} = 2 + \frac{1}{\frac{29}{9}} = 2 + \frac{1}{3+\frac{1}{\frac{9}{2}}} = 2 + \frac{1}{3+\frac{1}{4+\frac{1}{2}}} = [2,3,4,2]$$

$$\frac{29}{67} = 0 + \frac{1}{\frac{67}{29}} = [0,2,3,4,2]\ .$$

Este hecho se generaliza trivialmente obteniendo el siguiente resultado:

Proposición 8. *Sea $p, q \in \mathbb{Z}$, $p > q > 0$ y supongamos que*

$$\frac{p}{q} = [a_1, a_2, \ldots, a_n]\ .$$

Entonces

$$\frac{q}{p} = [0, a_1, a_2, \ldots, a_n]\ .$$

Nótese que $x = [a_1, \ldots, a_n]$ es negativo si y solo si $a_1 < 0$ y $0 < x < 1$ si y solo si $a_1 = 0$, y $x > 1$ equivale a $a_1 > 0$. Por otro lado el enunciado de la proposición no es cierto si $x = \frac{p}{q} < 0$. Por ejemplo,

$$\frac{-7}{2} = -4 + \frac{1}{2} = [-4, 2]$$

$$\frac{-2}{7} = -1 + \frac{5}{7} = [-1, 1, 2, 2].$$

Observación 5. Veamos si la descomposición de $\frac{67}{29}$ es única. Mediante el metodo de obtención de dicha fracción continua es único, pero si cambiamos el último término, tenemos que $a_4 = 2$ y puedo escribir

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

y por lo tanto escribir

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

De forma general, supongamos que $x \in \mathbb{Q}$ se escribe como la fracción continua $x = [a_1, \ldots, a_n]$. Si tenemos que $n \geq 2$ y $a_n \geq 2$ podemos escribir $a_n = (a_n - 1) + \frac{1}{1}$ y por lo tanto $[a_1, a_2, \ldots, a_n] = [a_1, a_2, \ldots, a_n - 1, 1]$ como números racionales. De la misma forma, la fracción continua $[b_1, \ldots, b_m, 1]$ representa el mismo número racional que $[b_1, \ldots, b_m + 1]$. Este hecho permite que, ocasionalmente, podamos suponer que la longitud de la representación de un racional es par o impar según convenga. Por otro lado obliga a que, si se quiere tener una representación única $[a_1, \ldots, a_n]$ para un racional x, tendremos que añadir la condición $a_n \geq 2$ siempre que $n \geq 2$:

Teorema 8. *Hay una correspondencia biyectiva entre números racionales y fracciones continuas simples finitas* $[a_1, \ldots, a_n]$ *con la condición* $a_n \geq 2$.

Demostración. Basta demostrar que la representación de un número racional x como fracción continua es única. Supongamos que las dos fracciones simples finitas $[a_1, a_2, \ldots, a_n]$ y $[b_1, b_2, \ldots, b_m]$ representan el mismo número racional x, esto es:

$$x = [a_1, a_2, \ldots, a_n] = [b_1, b_2, \ldots, b_m], \quad \text{donde } a_k > 1, b_j > 1, k, m > 1$$

Veamos entonces que ambas fracciones son la misma, es decir, que $n = m$ y $a_i = b_i, i = 1, 2, \ldots$.

Si $n = 1$, entonces $x \in \mathbb{Z}$ y por lo tanto también $m = 1$ y $a_1 = b_1$. Si $n, m > 1$, tendremos $x = a_1 + \frac{1}{[a_2,\ldots,a_n]} = b_1 + \frac{1}{[b_2,\ldots,b_m]}$. Puesto que $[a_1, \ldots, a_n]$ y $[b_1, \ldots, b_m]$ sean mayores que 1, necesariamente $a_1 = \lfloor x \rfloor$ y $b_1 = \lfloor x \rfloor$. Por lo tanto $a_1 = b_1$. Como consecuencia también $[a_2, \ldots, a_n] = [b_2, \ldots, b_m]$ y podemos continuar el proceso inductivamente. Por tanto $n = m$ y $a_2 = b_2, a_3 = b_3, \ldots, a_n = b_m$.

□

Nota 6. A partir del Teorema anterior no distinguiremos el número racional x de su representación como fracción continua $[a_1, \ldots, a_n]$, de manera que usaremos la expresión: " sea $x = [a_1, \ldots, a_n]$ una fracción continua finita simple" y entendemos que $x \in \mathbb{Q}$.

Dada la fracción continua finita simple $x = [a_1, \ldots, a_n]$, su i-ésimo convergente $(1 \leq i \leq n)$ $c_i = [a_1, \ldots, a_n]$ es también un número racional y los números p_i y q_i son enteros. De hecho, la proposición 7 implica (por el Teorema de Bezout) que p_i y q_i son primos entre si. Por tanto la igualdad $c_i = \frac{p_i}{q_i}$ expresa el número racional c_i como fracción irreducible. Obsérvese también que $q_i \geq 0$ $\forall i$, $q_i > 0$ si $i \geq 1$ y $q_1 < q_2 < \ldots < q_i < q_{i+1} < \ldots < q_n$.

La ecuación diofántica $ax + by = c$

Vamos a ver ahora como usar las fracciones continuas simples finitas en la resolución de ecuaciones diofánticas:

Vamos a considerar la ecuación diofántica $aX + bY = c$ donde $a, b, c \in \mathbb{Z}$ dados y donde el objetivo es calcular todas las soluciones enteras, es decir los pares $(x, y) \in \mathbb{Z}\text{x}\mathbb{Z}$ tales que $ax + by = c$. Como $\{aX + bY / X, Y \in \mathbb{Z}\}$ es el ideal $(a, b) \subset \mathbb{Z}$, si $d = m.c.d(a, b) > 0$, se tiene que $(a, b) = (d)$ y si $c \in (a, b), c \in (d)$ y $d|c$. Por tanto podemos escribir

$$d(\frac{a}{d}x + \frac{b}{d}y) = c$$

,tenemos $d(a'X + b'Y) = c$ y hay solución si y solo si $d|c$.

Ahora bien sean a', b', c' el resultado de dividir a, b, c por d, tenemos por tanto

$$d(a'x + b'y) = dc'$$

y la ecuación inicial se reduces a esta, de manera que $m.c.d(a', b') = 1$, por lo que podemos suponer que a, b son primos entre si.

Teorema 9. *La ecuación $ax + by = c$, donde a y b son enteros y primos entre sí, tiene un número infinito de soluciones enteras $(x, y) \in \mathbb{Z}^2$.*

Demostración. Primero vamos a ver la solución de la ecuación diofántica $ax+by = 1$, para ello primero expresamos $\frac{a}{b}$ como una fracción continua simple finita

$$\frac{a}{b} = [a_1, a_2, \ldots, a_n]$$

Usando que si $a_n \geq 2$ $[a_1, \ldots, a_n] = [a_1, \ldots, a_{n-1}, a_n - 1, 1]$ podemos suponer que n es par. Es claro que $\frac{a}{b} = \frac{p_n}{q_n}$ con $q_n > 0$, y ya sabemos que

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

a) Si $b > 0$, entonces $b = q_n$ y $a = p_n$, por tanto tenemos que

$$aq_{n-1} - p_{n-1} b = 1$$

y una solución particular de la ecuación será

$$(x, y) = (q_{n-1}, -p_{n-1}).$$

b) Si $b < 0$, entonces $b = -q_n$, $a = -p_n$, y se tiene

$$-aq_{n-1} + bp_{n-1} = 1$$

por lo que una solución particular de la ecuación diofántica será

$$(x, y) = (-q_{n-1}, p_{n-1}).$$

Supongamos ahora que (x_0, y_0),(x_1, y_1) son dos soluciones de la ecuación diofántica $ax + by = 1$, tenemos por tanto

$$ax_0 + by_0 = 1 \qquad ax_1 + by_1 = 1$$

$$a(x_0 - x_1) + b(y_0 - y_1) = 0$$

$$a(x_0 - x_1) = b(y_0 - y_1).$$

Con lo que llegamos a que como a y b son primos entre sí, a divide a $(y_1 - y_0)$ y podemos escribir

$$y_1 - y_0 = ta \quad t \in \mathbb{Z}$$

y sustituyendo $x_0 - x_1 = tb$ tendremos que:

$$x_1 = x_0 - tb$$
$$y_1 = y_0 + ta$$

para todo $t \in \mathbb{Z}$. Evidentemente, dada la solución (x_0, y_0), para cualquier $k \in \mathbb{Z}$, $(x_0 - kb, y_0 + kb)$ es también una solución. Por lo tanto tenemos infinitas soluciones a la ecuación $aX + bY = 1$. Ahora es fácil ver las soluciones enteras de la ecuación

$ax - by = c$, ya que si (x_0, y_0) es una solución particular de la ecuación $ax + by = 1$, solo basta con multiplicar por c en ambos lados de manera que tenemos

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

y la solución general de la ecuación diofántica será:

$$x = cx_0 - tb$$
$$y = cy_0 + ta$$

para todo $t \in \mathbb{Z}$.

□

Ejemplo 13. Encontrar una solución entera a la ecuación $205x - 93y = 1$, donde los enteros $205 = 5 \cdot 41$ y $93 = 3 \cdot 31$ son coprimos , por lo que la ecuación tiene solución.

Para resolverla vemos que se representa por la fracción continua $\frac{205}{93} = [2, 4, 1, 8, 2]$. Como tiene un número impar de cocientes parciales, escribiremos

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

que es equivalente a la anterior y tiene un número par de cocientes. Realizamos ahora

i	-1	0	1	2	3	4	5	6
a_i			2	4	1	8	1	1
p_i	0	1	2	9	11	97	108	205
q_i	1	0	1	4	5	44	49	93
c_i			$\frac{2}{1}$	$\frac{9}{4}$	$\frac{11}{5}$	$\frac{97}{44}$	$\frac{108}{49}$	$\frac{205}{93}$

Aquí $n = 6$, $p_{n-1} = p_5 = 108 = y_0$, $q_{n-1} = q_5 = 49 = x_0$, y por lo tanto, la solución de la ecuación general $205x - 93y = 1$ es

$x = x_0 + tb = 49 + 93t$ $\qquad$ $y = y_0 + tb = 108 + 205t$ $\qquad$ $t = 0, \pm 1, \pm 2, \ldots$

2.3. Fracciones continuas infinitas

En esta sección extenderemos el concepto de fracción continua simple finita al caso infinito.

Definición 13. Una fracción continua simple infinita es una sucesión de números enteros $\{a_n\}_{n=1}^{\infty}$ de manera que $a_k > 0$ para todo $k > 1$. La expresaremos mediante $[a_1, a_2, \ldots]$.

Nótese que para la fracción continua simple infinita $[a_1, a_2, \ldots]$, para cada $k \geq 0$ están definidos los enteros p_k y q_k, y el k-ésimo convergente $c_k = [a_1, \ldots, a_k] \in \mathbb{Q}$ (ya que su construcción solo depende de $a_1, \ldots, a_k$). Usando las propiedades que ya conocemos observamos que, por la Proposición 7, $c_2 - c_1 = \frac{1}{q_2 q_1} > 0$ y que

$c_3 - c_2 = \frac{-1}{q_3 q_2} < 0$. Por lo tanto se tiene $c_2 > c_1$ y $c_3 < c_2$. Aplicando la misma proposición tenemos que

$$c_3 - c_1 = \frac{a_3(-1)^2}{q_3 q_1} = \frac{a_3}{q_1 q_3} > 0.$$

Por lo tanto $c_1 < c_3 < c_2$. Estos resultados se generalizan fácilmente proporcionando el siguiente comportamiento de la sucesión de convergentes:

1. $c_1 < c_3 < c_5 < \ldots$ y $c_2 > c_4 > c_6 > \ldots$.

2. Para $k \in \mathbb{N}$, $c_{2k} > c_{2l+1}$ y $c_{2k+1} < c_{2l}$ para todo $l \in \mathbb{N}$.

3. c_{k+1} está comprendido entre c_{k-1} y c_k.

Teorema 10. *Sea $\{a_i\}_{i\geq 1}$ una sucesión de números enteros infinita, con $a_i \geq 1$ para todo $i > 1$, y sea $c_i = [a_1, \ldots, a_i]$. Entonces la sucesión $(c_i)_{i=1}^{\infty}$ converge.*

Demostración. Acabamos de ver en la observación anterior que los convergentes están ordenados de la siguiente manera:

$$c_1 < c_3 < c_5 < \ldots < c_{2n+1} < \ldots < c_{2n} < \ldots < c_6 < c_4 < c_2$$

Por tanto $c_2 > c_4 > c_6 > \ldots > c_{2i} \ldots$ con $i \in \mathbb{N}$ y todos ellos son mayores que c_1. Por tanto la sucesión $(c_{2i})_{i\geq 1}$ es decreciente y esta acotada inferiormente, por lo tanto converge. Sea ahora

$$\lim_{k\to\infty} c_{2k} = \alpha_1$$

Además $c_1 < c_3 < c_5 < \ldots < c_{2i+1} < \ldots$, todos ellos menores que c_{2k},para todo $k \in \mathbb{N}$, en particular menores que c_2. Entonces la sucesión $(c_{2i+1})_{i\geq 0}$ es creciente y acotada, por tanto converge y sea por tanto

$$\lim_{k\to\infty} c_{2k+1} = \alpha_2$$

Veamos que si ambos límites coinciden. Nótese que $\alpha_2 \leq \alpha_1$, como $a_i \geq 1$ para todo $i \geq 2$ y $q_0, q_1 \geq 1$, razonando por inducción sobre j llegamos a que

$$q_j = a_j q_{j-1} + q_{j-2} \geq j - 1 \quad \forall j \geq 1$$

Por tanto

$$c_{2i+1} - c_{2i} = \frac{1}{q_{2i+1} q_{2i}} \leq \frac{1}{2i(2i-1)},$$

que tiende a cero cuando i tiende a infinito. Por tanto, ambas sucesiones convergen al mismo límite, $\alpha = \alpha_1 = \alpha_2$ con

$$\lim_{k\to\infty} c_k = \alpha.$$

□

Sea $x \in \mathbb{R} \setminus \mathbb{Q}$ un número irracional, usaremos la construcción hecha al comienzo del capítulo de una fracción continua asociadaa x. Sea $x_1 = x$ y tomamos $a_1 = \lfloor x \rfloor$. Tenemos $x = a_1 + (x_1 - a_1) = a_1 + \frac{1}{(1/x_1 + a_1)}$. Definamos entonces $x_2 = \frac{1}{x_1 - a_1} \in \mathbb{R}$, $x_1 > 1$. Nótese que $x = [a_1, x_2]$. Sea $k > 1$ y supongamos construidos $a_1, \ldots, a_{k-1} \in \mathbb{Z}$, con $a_i > 1 \ \forall i \geq 2$ y números reales $x_1, \ldots, x_k$ con $x_2, \ldots, x_k > 1$ de manera que $x = [a_1, \ldots, a_{k-1}, x_k]$. Definimos:

$$a_k = \lfloor x_k \rfloor \quad x_{k+1} = \frac{1}{x_k - a_k}$$

Es evidente que $a_k \geq 1$, $x_{k+1} \in \mathbb{R}$ y $x_{k+1} > 1$. (Obsérvese que $x_k \neq a_k$, ya que $x_k \notin \mathbb{Q}$). También se tiene:

$$x = [a_1, \ldots, a_k, x_{k+1}] \ .$$

De esta forma construimos inductivamente una fracción continua simple infinita $[a_1, a_2, \ldots]$ asociada a x. Obsérvese que se tiene también que la fracción continua asociada a x_k es $[a_k, a_{k+1}, \ldots]$.

Proposición 9. *En las condiciones y con las restricciones anteriores. Sea c_k el k-ésimo convergente de $x = [a_1, \ldots, a_k, \ldots]$. Se tiene que $c_{2k+1} < x < c_{2k} \quad \forall k \geq 1$. Como consecuencia*

$$x = \lim_{k \to \infty} c_k$$

.

Demostración. Dado que $c_1 = a_1 < x$ y que $a_2 = \lfloor x_2 \rfloor < x_2$ tenemos que $x = a_1 + \frac{1}{x_2} < a_1 + \frac{1}{a_2} = c_2$. Por tanto $c_1 < x < c_2$. Supongamos, por inducción, que el resultado es cierto para los convergentes $d_1, \ldots, d_{2k}$ de cualquier fracción continua simple $[b_1, \ldots, b_n, \ldots]$ asociada a z, es decir supongamos que $d_{2k-1} < z < d_{2k}$, y apliquemos esta hipótesis a la fracción $[a_2, \ldots, a_n, \ldots]$ asociada a x_2. Tendremos entonces $d_{2k-1} < x_2 < d_{2k}$. Ahora, observemos que $c_j = a_1 + \frac{1}{d_{j-1}} \ \forall j \geq 2$ y por tanto

$$c_{2k+1} = a_1 + \frac{1}{d_{2k}} < a_1 + \frac{1}{x_2} = x < a_1 + \frac{1}{d_{2k-1}} = c_{2k}.$$

Evidentemente, la condición $c_{2k+1} < x < c_{2k} \ \forall k$ implica que $\lim c_{2k+1} \leq x \leq \lim c_{2k}$ y por tanto $\lim_{k \to \infty} c_k = x$.

□

Nota 7. La proposición anterior pretende identificar de forma unívoca un número irracional $x \in \mathbb{R} \setminus \mathbb{Q}$ con su fracción continua simple $[a_1, \ldots, a_n, \ldots]$. Recíprocamente, cualquier fracción continua simple (infinita) $[b_1, \ldots, b_n, \ldots]$ define el número real $\lim_{k \to \infty}([b_1, \ldots, b_k]) = y$ ambas construcciones son inversas una de la otra. Con la biyección que ya conocemos para los racionales tenemos que:

Teorema 11. *Existe una biyección entre el conjunto de los números reales y el conjunto de las fracciones continuas simples (finitas o infinitas).*

Ejemplo 14. Escribiremos $\sqrt{2}$ como una fracción continua simple infinita. El mayor entero menor que $\sqrt{2}$ es $a_1 = 1$, por tanto

$$\sqrt{2} = a_1 + \frac{1}{x_2} = 1 + \frac{1}{x_2}$$

Tenemos que $x_2 = \frac{1}{(\sqrt{2}-1)}$, es decir:

$$x_2 = \frac{1}{\sqrt{2}-1} \cdot \frac{\sqrt{2}+1}{\sqrt{2}+1} = \sqrt{2}+1$$

Por lo que

$$\sqrt{2} = a_1 + \frac{1}{x_2} = 1 + \frac{1}{1+\sqrt{2}}$$

El mayor entero menor que x_2 es $a_2 = 2$ por lo tanto

$$x_2 = a_2 + \frac{1}{x_3} = 2 + \frac{1}{x_3}$$

donde

$$x_3 = \frac{1}{x_2 - 2} = \frac{1}{\sqrt{2}-1} = \sqrt{2}+1 > 1$$

Hasta aquí tenemos

$$\sqrt{2} = 1 + \frac{1}{2 + \frac{1}{x_3}} = 1 + \frac{1}{2 + \frac{1}{\sqrt{2}+1}}$$

Ya que $x_3 = \sqrt{2}+1 = x_2$, se tendrá que $x_4 = x_5 = x_6 = \cdots$ iguales a $\sqrt{2}+1$. Por tanto tenemos que $\sqrt{2} = [1, 2, 2, 2, 2, \ldots]$

Si partimos de $x = [1, 2, 2, 2, 2, \ldots]$ veamos si llegamos a que representa $x = \sqrt{2}$. Tenemos que

$$x - 1 = \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \ddots}}},$$

tenemos entonces que

$$x = 1 + \frac{1}{2 + \left(\cfrac{1}{2 + \cfrac{1}{2 + \ddots}} \right)} = 1 + \frac{1}{2 + (x-1)} = 1 + \frac{1}{x+1},$$

de donde vemos que $x - 1 = \frac{1}{x+1}$ y tenemos $(x-1)(x+1) = 1$, es decir $x^2 = 2$. Por lo tanto $x = \sqrt{2}$, ya que $x > 0$.

2.4. Fracciones continuas periódicas

El ejemplo anterior nos da pie para ver qué sucede cuando la fracción continua es "periódica".

Definición 14. Una fracción continua periódica es una fracción continua simple de la forma

$$[a_1, a_2, \ldots, a_n, \overline{a_{n+1}, a_{n+2}, \ldots, a_{n+m}}] \,,$$

donde n y m son enteros con $n \geq 0$ y $m \geq 1$. El periodo es la sucesión de los términos $a_{n+1}, a_{n+2}, \ldots, a_{n+m}$ que se repiten indefinidamente y la longitud del periodo es m. Si $n = 0$ se dice que la fracción continua es periódica pura.

Definición 15. Se dice que un número es un irracional cuadrático si es una solución irracional de una ecuación cuadrática $ax^2 + bx + c = 0$ con a, b, c enteros y $a \neq 0$.

Teorema 12. *Toda fracción continua periódica representa un irracional cuadrático.*

Demostración. Sea $x = [a_1, a_2, \ldots, a_n, \overline{a_{n+1}, a_{n+2}, \ldots, a_{n+m}}]$ una fracción continua periódica. Entonces podemos expresar $x = [a_1, \ldots, a_n, y]$ con

$$y = [\overline{a_{n+1}, a_{n+2}, \ldots, a_{n+m}}] \,.$$

Como $y = [a_{n+1}, a_{n+2}, \ldots, a_{n+m}, \overline{a_{n+1}, a_{n+2}, \ldots, a_{n+m}}]$ tengo entonces que $y = [a_{n+1}, a_{n+2}, \ldots, a_{n+m}, y]$. Sea $c_i = \frac{p_i}{q_i}$ el i-ésimo convergente de la expresión de y como fracción continua, entonces:

$$y = \frac{yp_m + p_{m-1}}{yq_m + q_{m-1}}$$

y por lo tanto:

$$q_m y^2 + y(q_{m-1} - p_m) - p_{m-1} = 0.$$

Con lo que llegamos a que y es un número irracional cuadrático, ya que satisface una ecuación de segundo grado con coeficientes enteros. Por los resultados del Capítulo 1, sabemos que existe $d \in \mathbb{Z}$, $d > 1$ libre de cuadrados de manera que $y \in \mathbb{Q}(\sqrt{d})$, por tanto existen r, s números racionales únicos tales que $y = r + s\sqrt{d}$.

Por otra parte, como $x = [a_1, \ldots, a_n, y]$, sabemos que

$$x = \frac{yp'_n + p'_{n-1}}{yq'_n + q'_{n-1}}$$

donde $\frac{p'_n}{q'_n}$ y $\frac{p'_{n-1}}{q'_{n-1}}$ son los últimos convergentes para $[a_1, \ldots, a_n]$.

Puesto que $y \in \mathbb{Q}(\sqrt{d})$, y $p'_{n-1}, p'_n, q'_{n-1}, q'_n$ son enteros también $x \in \mathbb{Q}(\sqrt{d})$, ya que $\mathbb{Q}(\sqrt{d})$ es un cuerpo.

Es decir, $x = r' + s'\sqrt{d}$ con $r', s' \in \mathbb{Q}$. Además $s' \neq 0$ pues x está representado por una fracción continua simple infinita, por lo tanto x es un irracional cuadrático y toda fracción continua periódica representa un irracional cuadrático.

□

Teorema 13. *Si $a_1, a_2, \ldots, a_n$ son enteros positivos, la fracción continua periódica pura*

$$\alpha = [\overline{a_1, a_2, \ldots, a_n}]$$

es mayor que 1 y es un número irracional cuadrático. Sea $\beta = [\overline{a_n, a_{n-1}, \ldots, a_1}]$ entonces $\alpha' = \frac{-1}{\beta}$ es la segunda raíz, o la raíz conjugada, de la ecuación cuadrática que satisface α, y α' está entre -1 y 0.

Demostración. La primera parte del teorema ya la vimos en el teorema anterior, veamos la segunda parte. Tenemos que:

$$[a_1, a_2, \ldots, a_n] = \frac{p_n}{q_n}$$

con $p_n = a_n p_{n-1} + p_{n-2}$ y tenemos que $\frac{p_n}{p_{n-1}} = a_n + \frac{1}{\frac{p_{n-1}}{p_{n-2}}}$ y razonando por inducción tenemos que $\frac{p_{n-1}}{p_{n-2}} = [a_{n-1}, \ldots, a_1]$ y por tanto $\frac{p_n}{p_{n-1}} = [a_n, a_{n-1}, \ldots, a_1]$.

Sea ahora p'_i, q'_i los enteros correspondientes a la fracción continua $[a_n, \ldots, a_1]$. Tendremos entonces

$$\frac{p_n}{p_{n-1}} = \frac{p'_n}{q'_n}.$$

Razonando de la misma forma con $q_n = a_n q_{n-1} + q_{n-2}$ tendremos que

$$\frac{q_n}{q_{n-1}} = [a_n, a_{n-1}, \ldots, a_2] = \frac{p'_{n-1}}{q'_{n-1}}$$

Puesto que en este caso todos son periódicos tendremos que:

$$p'_n = p_n \qquad p'_{n-1} = q_n$$
$$q'_n = p_{n-1} \qquad q'_{n-1} = q_{n-1}$$

Recordemos que la ecuación cuadrática obtenida en el teorema anterior para α es:

$$q_n\alpha^2 - (p_n - q_{n-1})\alpha - p_{n-1} = 0$$

Sea ahora $\beta = [\overline{a_n, a_{n-1}, \ldots, a_1}]$ tenemos que

$$\beta = \frac{\beta p'_n + p'_{n-1}}{\beta q'_n + q'_{n-1}} = \frac{\beta p_n + q_n}{\beta p_{n-1} + q_{n-1}}$$

y por lo tanto β satisface la ecuación $p_{n-1}\beta^2 - (p_n - q_{n-1})\beta - q_n = 0$, que es equivalente a la ecuación:

$$q_n(\frac{-1}{\beta})^2 - (p_n - q_{n-1})(\frac{-1}{\beta}) - p_{n-1} = 0$$

Por tanto la ecuación cuadrática $q_n x^2 - (p_n - q_{n-1})x - p_{n-1} = 0$ tiene dos raíces $x_1 = \alpha$ y $x_2 = \frac{-1}{\beta}$. Como β representa la fracción periódica pura $[\overline{a_n, a_{n-1}, \ldots, a_1}]$, donde $a_n, a_{n-1}, \ldots, a_1$ son todos enteros positivos, entonces tenemos $\beta > 1$, $0 < \frac{1}{\beta} < 1$, y por tanto $-1 < \frac{-1}{\beta} < 0$.

□

Definición 16. Un irracional cuadrático α se dice que es reducido si α es mayor que 1 y su conjugado $\overline{\alpha}$, está entre -1 y 0.

Nota 8. Sea $D \in \mathbb{Z}$, $D > 0$ con $\sqrt{D} \in \mathbb{R}_+$ irracional, es decir D no es un cuadrado perfecto, y $\alpha = \frac{p+\sqrt{D}}{q}$ con $p, q \in \mathbb{Z}$, $q > 0$. El conjugado de α es $\overline{\alpha} = \frac{p-\sqrt{D}}{q}$. Supongamos que α es reducido, es decir $\alpha > 1$ y $-1 < \overline{\alpha} < 0$. Puesto que $\alpha + \overline{\alpha} > 0$ se tiene que $\frac{2p}{q} > 0$ y por tanto $p > 0$. Por otro lado $\overline{\alpha} = \frac{p-\sqrt{D}}{q} < 0$ implica $p < \sqrt{D}$. Así pues tendremos

$$0 < p < \sqrt{D}.$$

La desigualdad $\alpha > 1$ implica que $p + \sqrt{D} > q$ y la desigualdad $\overline{\alpha} > -1$ que $p - \sqrt{D} > -q$, es decir $q > \sqrt{D} - p > 0$. Por lo tanto $\sqrt{D} - p < q < \sqrt{D} + p$. Como consecuencia tenemos:

Lema 4. *Sea $D \in \mathbb{Z}$, $D > 0$ con $\sqrt{D}$ irracional. Entonces hay solo un número finito de racionales cuadráticos reducidos de la forma $\frac{p+\sqrt{D}}{q}$ con $p, q \in \mathbb{Z}$, $q > 0$.*

Sea $\alpha > 1$ un irracional cuadrático reducido, α es raíz de una ecuación cuadrática de la forma $ax^2 + bx + c = 0$ con a, b, c enteros, $a > 0$. Tenemos entonces

$$\alpha = \frac{-b + \sqrt{b^2 - 4ac}}{2a} = \frac{k + \sqrt{D}}{h}$$

con $D = b^2 - 4ac > 0$ el discriminante, $h = 2a$ y $k = -b$. Puesto que α es reducido, también $\overline{\alpha} = \frac{k-\sqrt{D}}{h} \in (-1, 0)$.

Sea $a_1 = \lfloor x \rfloor$ y $\alpha_1 = \frac{1}{\alpha - a_1}$. Nótese que $\alpha = a_1 + \frac{1}{\alpha_1}$. Tenemos entonces:

Lema 5. *α_1 es un irracional cuadrático reducido de la forma $\alpha_1 = \frac{k_1+\sqrt{D}}{h_1}$.*

Demostración. Sabemos que $a\alpha^2 + b\alpha + c = 0$, sustituyendo $\alpha = a_1 + \frac{1}{\alpha_1}$ tendremos:

$$a\Big(a_1 + \frac{1}{\alpha_1}\Big)^2 + b\Big(a_1 + \frac{1}{\alpha_1}\Big) + c = 0$$

operando en esta ecuación obtenemos:

$$a(\alpha_1 a_1 + 1)^2 + b\alpha_1(a_1\alpha_1 + 1) + c\alpha_1^2 = 0$$

y por tanto $A\alpha_1^2 + B\alpha_1 + c = 0$, siendo $A = aa_1^2 + ba_1 + c$, $B = 2aa_1 + b$, $C = a$. El discriminante de esta ecuación es:

$$A^2 = B^2 - 4AC = (2a_1 a + b)^2 - 4c(a_1^2 a + ba_1 + c) \qquad = b^2 - 4ac = D$$

y como consecuencia

$$\alpha_1 = \frac{k_1 + \sqrt{D}}{h_1}$$

siendo $k_1 = -b - 2ca_1$, $h_1 = 2(aa_1^2 + ba_1 + c)$. Sabemos entonces que $\alpha_1 > 1$, la raíz conjugada de α_1 es:

$$\overline{\alpha_1} = \Big(\overline{\frac{1}{\alpha - a_1}}\Big) = \frac{1}{\overline{\alpha} - a_1}.$$

Como $a_1 \geq A$ y $\overline{\alpha} \in (-1, 0)$ tendremos que $a_1 - \overline{\alpha} > 1$ y por tanto $\overline{\alpha_1} > -1$. Es necesario ver que $\overline{\alpha_1} < 0$ y como consecuencia, $\overline{\alpha_1} \in (-1, 0)$ y α_1 es un irracional cuadrático reducido.

Observemos que también $\beta = \frac{-1}{\overline{\alpha}}$ es un irracional cuadrático reducido.

□

Teorema 14. *Si $\alpha > 1$ es un irracional cuadrático reducido, entonces la fracción continua para α es periódica pura.*

Demostración. La construcción de la fracción continua de α, $[a_1, \ldots, a_n, \ldots]$ calcula recursivamente $\alpha = \alpha_0, \alpha_1, \ldots$ irracionales cuadráticos y enteros $a_1, \ldots, a_n, \ldots$ de manera que $\alpha = [a_1, \ldots, a_n, \alpha_n]$, $a_{n+1} = \lfloor \alpha_n \rfloor$. Por el lema anterior, α_n es reducido y pertenece al conjunto:

$$I = \left\{ \beta = \frac{p + \sqrt{D}}{q} \quad : \quad q > 0; \beta \text{ reducido} \right\}$$

Por el Lema 4, I es un conjunto finito, por tanto existen k, l, $k < l$ mínimos con $\alpha_k = \alpha_l$. El Teorema se deduce entonces de las siguientes afirmaciones:

i) Si $\alpha_k = \alpha_l$ entonces $\alpha_{k+i} = \alpha_{l+i}$ $\forall i \geq 0$.

ii) $k = 0$.

Para probar i) es suficiente demostrar que si $\alpha_k = \alpha_l$, entonces $\alpha_{k+1} = \alpha_{l+1}$. Puesto que

$$\alpha_k = a_{k+1} + \frac{1}{\alpha_{k+1}} = \alpha_l = a_{l+1} + \frac{1}{\alpha_{l+1}}$$

y, como a_{k+1} y a_{l+1} son los mayores enteros menores que α_k y α_l respectivamente se tiene que $a_{k+1} = a_{l+1}$ y por tanto para $\alpha_{k+1} = \alpha_{l+1}$.

Podemos repetir el mismo argumento para $\alpha_{k+2} = \alpha_{l+2}, \alpha_{k+3} = \alpha_{l+3}, \ldots$

Para probar ii) veamos que $\alpha_k = \alpha_l$ implica que $\alpha_{k-1} = \alpha_{l-1}$. Para esto, usaremos los conjugados de los cocientes completos α_k y α_l obteniendo $\overline{\alpha_k} = \alpha$ se tiene

$$\beta_k = \frac{-1}{\overline{\alpha_k}} = \frac{-1}{\overline{\alpha_l}} = \beta_l$$

Ahora si $k \neq 0$, tenemos

$$\alpha_{k-1} = a_k + \frac{1}{\alpha_k} \qquad y \qquad \alpha_{l-1} = a_l + \frac{1}{\alpha_l}$$

tomamos conjugados

$$\overline{\alpha_{k-1}} = a_k + \frac{1}{\overline{\alpha_k}} \qquad y \qquad \overline{\alpha_{l-1}} = a_l + \frac{1}{\overline{\alpha_l}}$$

y por tanto

$$-\frac{1}{\overline{\alpha_k}} = a_k - \overline{\alpha_{k-1}} \qquad y \qquad -\frac{1}{\overline{l}} = a_l - \overline{l-1}$$

que es lo mismo que

$$\beta_k = a_k + \frac{1}{\beta_{k-1}} \qquad y \qquad \beta_l = a_l + \frac{1}{\beta_{l-1}}$$

Ya que $\alpha_{k-1}, \alpha_{l-1}$ son reducidos, tenemos

$$-1 < \overline{\alpha_{k-1}} < 0 \qquad y \qquad -1 < \overline{\alpha_{l-1}} < 0$$

por tanto

$$0 < -\overline{\alpha_{k-1}} = \frac{1}{\beta_{k-1}} < 1 \qquad y \qquad 0 < -\overline{\alpha_{l-1}} = \frac{1}{\beta_{l-1}} < 1$$

Llegamos a que a_k, a_l son los mayores enteros menores que β_k, β_l, respectivamente, y ya que $\beta_k = \beta_l$ se tiene que $a_k = a_l$ y por lo tanto

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

Por tanto $\alpha_k = \alpha_l$ implica $\alpha_{k-1} = \alpha_{l-1}$

Ahora bien si $k-1 \neq 0$, esto es, si α_k no es el primer cociente completo, repetimos el proceso k veces para probar que $\alpha_{k-k} = \alpha_0 = \alpha_{l-k} = \alpha_s$.

Por tanto si expresamos el irracional cuadrático como una fracción continua tenemos las ecuaciones:

$$\begin{aligned}
\alpha &= a_1 + \frac{1}{\alpha_1} \\
\alpha_1 &= a_2 + \frac{1}{\alpha_2} \\
\cdots \quad &\cdots \quad \cdots \\
\alpha_{s-2} &= a_{s-1} + \frac{1}{\alpha_{s-1}} \\
\alpha_{s-1} &= a_s + \frac{1}{\alpha_s} = a_s + \frac{1}{\alpha}
\end{aligned}$$

donde $\alpha, \alpha_1, \alpha_2, \ldots, \alpha_{s-1}$, son todos diferentes, y donde $\alpha_s = \alpha$, esto es, donde se repite α.

Ya que para cada $\alpha_k > 1$, existe exactamente un mayor entero a_k menor que α_k, es claro que la sucesión $a_1, a_2, \ldots, a_s$ se repetirá:

$$\alpha_s = a_{s-1} + \frac{1}{\alpha_{s+1}} = \alpha_0 = a_1 + \frac{1}{\alpha_1}$$

Por tanto la fracción continua para α tendrá la forma

$$\alpha = [\overline{a_1, a_2, \ldots, a_s}]$$

que es una fracción periódica pura.

□

Teorema 15. ***(de Lagrange)*** *Cualquier número irracional cuadrático α se puede expresar como una fracción continua que es periódica de un punto en adelante.*

Demostración. Sea la expresión de α

$$\alpha = [a_1, a_2, \ldots, a_{n+1}, \alpha_{n+1}].$$

Entonces sabemos que

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

donde α y α_{n+1} son irracionales cuadráticos y $\alpha_{n+1} > 1$. Tomando conjugados a ambos lados de la ecuación tenemos

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

y despejando $\overline{\alpha_{n+1}}$

$$\overline{\alpha_{n+1}} = -\frac{\overline{\alpha}q_{n-1} - p_{n-1}}{\overline{\alpha}q_n - p_n} = \frac{-q_{n-1}}{q_n}\left(\frac{\overline{\alpha} - \frac{p_{n-1}}{q_{n-1}}}{\overline{\alpha} - \frac{p_n}{q_n}}\right) = \frac{-q_{n-1}}{q_n}\left(\frac{\overline{\alpha} - c_{n-1}}{\overline{\alpha} - c_n}\right)$$

donde $c_{n-1} = \frac{p_{n-1}}{q_{n-1}}$ y $c_n = \frac{p_n}{q_n}$. Puesto que $c_n \longrightarrow \alpha$ si $n \longrightarrow \infty$ tendremos

$$\lim_{n\to\infty} \frac{\overline{\alpha} - c_{n-1}}{\overline{\alpha} - c_n} = \frac{\overline{\alpha} - \alpha}{\overline{\alpha} - \alpha} = 1.$$

También sabemos que los convergentes c_n son alternativamente menores y mayores que α y por tanto la fracción $\frac{\overline{\alpha}-c_{n-1}}{\overline{\alpha}-c_n}$ será alternativamente mayor y menor que 1. También sabemos que q_n y q_{n-1} son ambos enteros positivos y que $0 < q_{n-1} < q_n$ por tanto $\frac{q_{n-1}}{q_n} < 1$.

Una vez encontrado un valor n que haga $\frac{\overline{\alpha}-c_{n-1}}{\overline{\alpha}-c_n}$ significativamente menor que 1, el valor de $\overline{\alpha_{n-1}} = \frac{-q_{n-1}}{q_n}\left(\frac{\overline{\alpha}-c_{n-1}}{\overline{\alpha}-c_n}\right)$ estará entre -1 y 0. Esto prueba que α_{n+1} es reducido , por el teorema anterior la fracción continua para α será periódica, desde ahí, y queda probado el teorema.

□

Capítulo 3

La ecuación de Pell

En este capítulo vamos a discutir las soluciones enteras x e y de la ecuación

$$x^2 - dy^2 = \pm 1$$

donde $d > 0$ es un entero, y además supondremos que d es un entero libre de cuadrados. A esta ecuación la llamaremos ecuación de Pell, el nombre de esta ecuación lo puso Euler, que la atribuyó a John Pell(1610-1685) por error ya que el estudio profundo de estas ecuaciones lo realizó Brouncker. Aunque Brouncker utilizó fracciones continuas y obtuvo soluciones, fue Lagrange el matemático que demostró que tenía infinitas soluciones.

Como ya sabemos del Capítulo 1 una solución de la ecuación de Pell $x^2-dy^2 = \pm 1$ proporciona una unidad $x+y\sqrt{d}$ del anillo $\mathbb{Z}[\sqrt{d}]$, no obstante las soluciones de dicha ecuación aparecen de forma distinta en problemas muy antiguos. Mencionaremos el que seguramente es el más famoso: el problema "bovino" (o del ganado) de Arquímedes:

El dios Sol tenía un rebaño formado por un cierto número de toros blancos, negros, moteados y amarillos, así como vacas de los mismos colores. De tal forma que:

- El número de toros blancos es la mitad y la tercera parte de los negros más los amarillos.
- El número de toros negros es igual a la cuarta más la quinta parte de los moteados más los amarillos.
- El número de toros moteados es igual a la sexta más la séptima parte de los blancos más los amarillos.
- El número de vacas blancas es igual a un tercio más un cuarto de la suma de los toros negros y las vacas negras.
- El número de vacas negras es igual a la cuarta parte más la quinta parte de la suma de los toros moteados más las vacas moteadas.
- El número de vacas moteadas es igual a la quinta más la sexta parte de la suma de los toros amarillos mas las vacas amarillas.

- El número de vacas amarillas es igual a la sexta más la séptima parte de la suma de los toros blancos más las vacas blancas.

Resolver el problema así planteado supone, según Arquímedes, un conocimiento avanzado de las matemáticas. No obstante, se añaden otras dos condiciones adicionales:

- La suma de los toros blancos y los negros es un número cuadrado.
- La suma de los toros moteados y amarillos es un número triangular.

El problema se resuelve mediante un sistema de 9 ecuaciones (dos de ellas cuadráticas y el resto lineales) con 10 incógnitas. Tras eliminar variables el problema se reduce a encontrar una solución de la ecuación

$$x^2 - 4729494y^2 = 1$$

con x e y enteros, ecuación que en su día Arquímedes no logró resolver.

En este capítulo d denota siempre un entero positivo libre de cuadrados. Ya sabemos (Capítulo 1) que hay infinitas unidades en $\mathbb{Z}[\sqrt{d}]$, de hecho si $\varepsilon = x + y\sqrt{d}$ es la menor solución mayor que 1 (la solución fundamental) se tiene que

$$\mathbb{Z}[\sqrt{d}]^* = \{\pm\varepsilon^n \quad : \quad n \in \mathbb{Z}\}.$$

Dado que hay infinitas unidades $\eta = x + y\sqrt{d}$ con $x, y > 1$, la expresión

$$x - y\sqrt{d} = \frac{\pm 1}{x + y\sqrt{d}}$$

tiende a 0 cuando x, y crecen. Por tanto la fracción $\frac{x}{y}$ debe "aproximarse" a $\sqrt{d}$. Esto nos lleva a analizar las aproximaciones racionales de $\sqrt{d}$ y el posible cálculo mediante los convergentes de la fracción continua de $\sqrt{d}$.

3.1. Cálculo de una solución

Una consecuencia de los resultados del capítulo anterior es:

Proposición 10. *Sea $m > 0$ un entero que no es un cuadrado perfecto entonces*

$$\sqrt{m} = [a_1, \overline{a_2, \ldots, a_n, 2a_1}]$$

donde $a_2, \ldots, a_n$ son simétricos, es decir, $a_2 = a_n$, $a_3 = a_{n-1}, \ldots$

Demostración. Si $m > 0$ es un entero que no es un cuadrado perfecto, la fracción continua para $\sqrt{m}$ tiene una forma interesante. Notese primero que $\sqrt{m} > 1$ y por tanto $-\sqrt{N}$ no pertenece a -1 y 0, por tanto $\sqrt{m}$ no es reducido y su fracción continua no es periódica pura.

Por otro lado, si a_1 es el mayor entero menor que $\sqrt{m}$, el número $\sqrt{m} + a_1$, es mayor que 1 y su conjugado $-\sqrt{m} + a_1$ está entre -1 y 0, por tanto $\sqrt{m} + a_1$ es reducido.

Si $\sqrt{m} = [a_1, \ldots, a_n, \ldots]$ tendremos que

$$\sqrt{m} + a_1 = [2a_1, a_2, \ldots]$$

y, ya que esta fracción es periódica pura, debe tener la forma:

$$\alpha = \sqrt{m} + a_1 = [\overline{2a_1, a_2, \ldots, a_n}] \ .$$

Por consiguiente, la fracción continua de $\sqrt{m}$ será

$$\sqrt{m} = [a_1, \overline{a_2, \ldots, a_n, 2a_1}]$$

donde el periodo empieza después del primer término y termina con el término $2a_1$.

Veamos dos ejemplos:

$$\sqrt{29} = [5, \overline{2, 1, 1, 2, 10}]$$
$$\sqrt{19} = [4, \overline{2, 1, 3, 1, 2, 8}] \ .$$

Nótese que, a excepción del término $2a_1$, la parte periódica es simétrica. La parte simétrica puede tener o no un término central.

Para ver más sobre la simetría, como ya hemos visto que si $\overline{\alpha} = -\sqrt{m} + a_1$ es el conjugado de $\alpha = a_1 + \sqrt{m}$, entonces la expresión de $\frac{-1}{\overline{\alpha}}$ es la misma que la de α pero con el periodo inverso. Por lo tanto, revertiendo el proceso se tiene

$$\frac{-1}{\overline{\alpha}} = \frac{1}{\sqrt{m} - a_1} = [\overline{a_n, \ldots, 2a_1}] \ .$$

Por otro lado, con la expresión de $\sqrt{m}$ restándole a_1 tendremos que

$$\sqrt{m} - a_1 = [0, \overline{a_2, \ldots, a_n, 2a_1}]$$

y el inverso de esta expresión

$$\frac{1}{\sqrt{m} - a_1} = [\overline{a_2, \ldots, a_n, 2a_1}]$$

Sabemos,sin embargo, que la expresión en una fracción continua es única, por lo tanto concluimos que

$$a_n = a_2, a_{n-1} = a_3, \ldots, a_3 = a_{n-1}, a_2 = a_n$$

Por tanto

$$\sqrt{m} = [a_1, \overline{a_2, a_3 \ldots, a_4, a_3, a_2, 2a_1}] \ .$$

□

Veamos que a partir de este resultado podemos ya encontrar una solución:

Teorema 16. *Sea $d > 1$ libre de cuadrados y supongamos que*

$$\sqrt{d} = [a_1, \overline{a_2, \ldots, a_n, 2a_1}].$$

Entonces $p_n^2 - dq_n^2 = (-1)^n$ y $p_{2n}^2 - dq_{2n}^2 = 1$. Como consecuencia, si n es impar $(x, y) = (p_n, q_n)$ es una solución de $x^2 - dy^2 = -1$ y (p_{2n}, q_{2n}) de $x^2 - dy^2 = 1$. Si n par $(x, y) = (p_n, q_n)$ es solución de $x^2 - dy^2 = 1$.

Demostración. La fracción continua de $\sqrt{d}$ es lo único necesario para resolver la ecuación $x^2 - dy^2 = \pm 1$. Sabemos que :

$$\sqrt{d} = [a_1, \overline{a_2, \ldots, a_n, 2a_1}] = [a_1, a_2, \ldots, a_n, \alpha_{n+1}]$$

donde

$$\alpha_{n+1} = [\overline{2a_1, a_2, \ldots, a_n}] = \sqrt{d} + a_1 \ .$$

Usaremos también que

$$\sqrt{d} = \frac{\alpha_{n+1} p_n + p_{n-1}}{\alpha_{n+1} q_n + q_{n-1}} \ ,$$

donde p_{n-1}, q_{n-1}, p_n y q_n son los enteros ya conocidos, que facilitan los convergentes $c_{n-1} = \frac{p_{n-1}}{q_{n-1}}$ y $c_n = \frac{p_n}{q_n}$ justo antes del término $2a_1$. Si sustituimos α_{n+1} obtenemos que

$$\sqrt{d} = \frac{(\sqrt{d} + a_1)p_n + p_{n-1}}{(\sqrt{d} + a_1)q_n + q_{n-1}},$$

por tanto

$$\sqrt{d}(\sqrt{d} + a_1)q_n + q_{n-1}\sqrt{d} = (\sqrt{d} + a_1)p_n + p_{n-1},$$

que es equivalente a

$$dq_n + (a_1 q_n + q_{n-1})\sqrt{d} = (a_1 p_n + p_{n-1}) + p_n\sqrt{d}.$$

Esta ecuación tiene la forma $a + b\sqrt{d} = c + d\sqrt{d}$ donde a, b, c, d son enteros y $\sqrt{d}$ es irracional, y esto implica que $a = c$ y $b = c$. Por tanto se tiene que $dq_n = a_1 p_n + p_{n-1}$ y $a_1 q_n + q_{n-1} = p_n$.

Despejando en estas ecuaciones p_{n-1} y q_{n-1} en términos de p_n y q_n tenemos

$$p_{n-1} = dq_n - a_1 p_n \qquad y \qquad q_{n-1} = p_n - a_1 q_n$$

Además por la igualdad ya conocida $p_n q_{n-1} - q_n p_{n-1} = (-1)^n$ y sustituyendo p_{n-1} y q_{n-1} de lo anterior tenemos

$$p_n(p_n - a_1 q_n) - q_n(dq_n - a_1 p_n) = (-1)^n$$

esto es

$$p_n^2 - dq_n^2 = (-1)^n.$$

Si n es par, esta ecuación será

$$p_n^2 - dq_n^2 = (-1)^n = 1$$

y por tanto, una solución particular de la ecuación de Pell $x^2 - dy^2 = 1$ será

$$x_1 = p_n \qquad\qquad y_1 = q_n.$$

Si n es impar, entonces $p_n^2 - dq_n^2 = (-1)^n = -1$ y una solución particular de la ecuación de Pell $x^2 - dy^2 = -1$ será $x_1 = p_n$ e $y_1 = q_n$.

Si n es impar y queremos encontrar una solución particular de la ecuación $x^2 - dy^2 = 1$, buscamos la solución en el segundo periodo de la fracción continua de $\sqrt{d}$ de este modo tomamos el término a_{2n} como sigue

$$\sqrt{d} = [a_1, \ldots, a_n, 2a_1, a_2, \ldots, a_n, 2a_1, \ldots]$$

por tanto el término a_n cuando aparece otra vez, es el término $2n$-ésimo, entonces

$$p_{2n}^2 - dq_{2n}^2 = (-1)^{2n} = 1$$

y $x_1 = p_{2n}$ e $y_1 = q_{2n}$ nos da una solución particular de la ecuación $x^2 - dy^2 = 1$.

Esto nos muestra que siempre podemos encontrar soluciones particulares a la ecuación $x^2 - dy^2 = 1$y alguna vez soluciones de la ecuación $x^2 - dy^2 = -1$. Esto se debe a que no todas la ecuaciones $x^2 - dy^2 = -1$ tienen soluciones enteras.

□

Ejemplo 15. Encontrar una solución particular de la ecuación $x^2 - 21y^2 = 1$.

Aquí $d = 21$, y la fracción continua es

$$\sqrt{21} = [4, \overline{1, 1, 2, 1, 1, 8}]$$

donde vemos que $a_n = a_6$, por tanto $n = 6$. y es un número par. Calculamos $c_6 = \frac{55}{12}$ y tenemos

$$x_1 = p_6 = 55 \qquad\qquad y_1 = q_6 = 12$$

y

$$x_1^2 - 21y_1^2 = 55^2 - 21 \cdot 12^2 = 3025 - 3024 = 1$$

por tanto son soluciones particulares de la ecuación.

La solución que calculamos en el Teorema es , de hecho, la solución fundamental, pero este hecho no es inmediato.

3.2. Aproximaciones racionales

Sea $\xi \in \mathbb{R} \setminus \mathbb{Q}$ irracional y $\xi = [a_1, a_2, \ldots]$ su desarrollo como fracción continua. Como ya sabemos la sucesión de convergentes $c_n = \frac{p_n}{q_n}$; $n \geq 1$ de ξ verifica que $\lim_{n\to\infty} c_n = \xi$. Veamos algunos resultados más precisos en esta sección:

Proposición 11. *Se tiene que:*

$$\frac{1}{q_n(q_n + q_{n+1})} < \left|\xi - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}}$$

y como consecuencia:

$$\left|\xi - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}.$$

Demostración. A partir de $\xi = [a_1, \ldots, a_n, \xi_{n+1}]$ con $\xi_{n+1} = [a_{n+1}, \ldots]$ sabemos que

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

Ahora en la expresión de $\xi - \frac{p_n}{q_n}$ obtenemos que

$$\left|\xi - \frac{p_n}{q_n}\right| = \frac{1}{q_n(q_n\xi_{n+1} + q_{n-1})}. \quad (*)$$

Usando las desigualdades :

$$q_{n+1} = a_{n+1}q_n + q_{n-1} < \xi_{n+1}q_n + q_{n-1} < q_n(a_n + 1) + q_{n-1} = q_{n+1} + q_n$$

en (*), se obtiene que

$$\frac{1}{q_n(q_n + q_{n+1})} < \left|\xi - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}}.$$

La segunda desigualdad del enunciado es inmediata ya que $q_n < q_{n+1}$.

□

El siguiente resultado precisa el alcance de los convergentes $\{c_n\}$ en base a proporcionar "buenas" aproximaciones de un número real.

Teorema 17. *(a) Sea ξ un número irracional y $c_i = \frac{p_i}{q_i}$, $i \in \mathbb{N}$, el i-ésimo convergente de la fracción continua simple de ξ. Si $r, s \in \mathbb{Z}$ con $s > 0$ y k es un entero positivo tal que*

$$|s\xi - r| < |q_k\xi - p_k| \ ,$$

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

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

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

entonces $\frac{r}{s}$ es un convergente de la fracción continua de ξ.

Demostración. (a) Razonemos por reducción al absurdo, suponiendo que $1 \leq y < q_{k+1}$. 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:

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

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

Ya es conocida la igualdad $p_k q_{k+1} - p_{k+1} q_k = (-1)^k$ del capitulo anterior, por lo que la solución del sistema esta dada por

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

$$y = (-1)^{k-1}(r q_k - s p_k) \ .$$

Probaremos que x e y son no nulos y tienen distinto 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 $q_{k+1}|s$,

$q_{k+1} \leq s$ lo cual es una contradicción. Supongamos ahora $y = 0$, entonces $r = p_k x$, $s = q_k x$, entonces

$$|s\xi - r| = |x||q_k\xi - p_k| \geq |q_k\xi - p_k|$$

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 $q_i > 0$, 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 impar, tenemos la siguiente condición

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

mientras que si k es par se tiene

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

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

$$\begin{aligned} |s\xi - r| &= |(q_k x + q_{k+1}y)\xi - (p_k x + p_{k+1}y)| \\ &= |x(q_k\xi - p_k) + y(q_{k+1}\xi - p_{k+1})| \\ &= |x||q_k\xi - p_k| + |y||q_{k+1}\xi - p_{k+1}| \qquad \geq |x||q_k\xi - p_k| \geq |q_k\xi - p_k| \end{aligned}$$

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

(b) Supongamos que $\frac{x}{y}$ no es un convergente de la fracción continua de ξ, es decir $\frac{x}{y} \neq \frac{p_i}{q_i}$ para todo i. Sea k el entero no negativo más grande tal que $y \geq q_k$ (entonces $y \geq q_0 = 1$ y $q_k \to \infty$ si $k \to \infty$). Entonces $q_k \leq s \leq q_{k+1}$ y por (a), tenemos

$$|q_k\xi - p_k| \leq |s\xi - r| = s\left|\xi - \frac{r}{s}\right| < \frac{1}{2s}\ ,$$

luego $\left|\xi - \frac{p_k}{q_k}\right| < \frac{1}{2sq_k}$. Como $\frac{r}{s} \neq \frac{p_k}{q_k}$, se tiene $|sp_k - rq_k| \geq 1$ así

$$\begin{aligned} \frac{1}{sq_k} \leq \frac{|sp_k - rq_k|}{sq_k} &= \left|\frac{p_k}{q_k} - \frac{r}{s}\right| = \left|\frac{p_k}{q_k} - \frac{r}{s} + \xi - \xi\right| \\ &\leq \left|\xi - \frac{p_k}{q_k}\right| + \left|\xi - \frac{r}{s}\right| < \frac{1}{2sq_k} + \frac{1}{2s^2} \end{aligned}$$

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

□

3.3. La solución general de la ecuación de Pell

Veamos en primer lugar que todas las soluciones de la ecuación $x^2 - dy^2 = \pm 1$ se pueden obtener a partir de los convergentes de la fracción continua de $\sqrt{d}$.

Teorema 18. *Sea k, d enteros con $d > 0$ libre de cuadrados y $|k| < \sqrt{d}$. Sea (x, y) una solución de la ecuación $x^2 - dy^2 = k$ con $x, y > 0$. Entonces $\frac{x}{y}$ es un convergente de $\sqrt{d}$.*

Demostración. Supongamos primero que k es positivo. Tendremos que:

$$0 < x - y\sqrt{d} = \frac{k}{x + y\sqrt{d}} < \frac{\sqrt{d}}{x + y\sqrt{d}} = \frac{1}{y(\frac{x}{y\sqrt{d}} + 1)}.$$

Como $x > y\sqrt{d}$ deducimos que:

$$\left|\frac{x}{y} - \sqrt{d}\right| < \frac{1}{2y^2}$$

y por el Teorema anterior $\frac{x}{y}$ es un convergente de $\sqrt{d}$. Supongamos ahora que k es negativo. A partir de la igualdad $y^2 - \frac{x^2}{d} = \frac{-k}{d}$ obtenemos:

$$0 < y - \frac{x}{\sqrt{d}} = \frac{-(\frac{k}{d})}{y + \frac{x}{\sqrt{d}}} < \frac{1}{y\sqrt{d} + x} = \frac{1}{x(1 + \frac{y\sqrt{d}}{x})}$$

y por tanto:

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

Como antes, esto implica que $\frac{x}{y}$ es un convergente de $\xi = \frac{1}{\sqrt{d}}$. Si $\sqrt{d} = [a_1, a_2, \ldots]$, es evidente que $\frac{1}{\sqrt{d}} = [0, a_1, a_2, \ldots]$y es inmediata para los convergentes de $\frac{1}{\sqrt{d}}$ (a partir del segundo) si $\{\frac{1}{c_n}\}_{n\geq 1}$ siendo $\{c_n\}$ los de $\sqrt{d}$.

□

Teorema 19. *Sea $\frac{p_n}{q_n}$ el n-ésimo convergente de la fracción continua de $\sqrt{d}$ con d entero. Entonces, $p_n + q_n\sqrt{d}$ es una unidad en $\mathbb{Z}[\sqrt{d}]$ si y solo si*

$$\sqrt{d} = [a_1, \overline{a_1, \ldots, a_n, 2a_1}]$$

Si esto ocurre, entonces $d(p_n + q_n\sqrt{d}) = (-1)^n$.

Demostración. Supongamos $p_n^2 - dq_n^2 = \pm 1$. Veamos primero como el signo depende de n. Hemos visto que $\sqrt{d}$ está entre los convergentes $\frac{p_n}{q_n}$ y $\frac{p_{n+1}}{q_{n+1}}$. Por lo tanto, el signo de $\frac{p_n}{q_n} - \sqrt{d}$ es el mismo que el de $\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}}$, y por la igualdad $p_{n+1}q_n - p_nq_{n+1} = (-1)^{n+1}$, el signo será $(-1)^n$. Por otro lado, $p_n + q_n\sqrt{d}$ es positivo, por tanto tenemos

$$p_n^2 - dq_n^2 = (p_n + q_n\sqrt{d})(p_n - q_n\sqrt{d}) = (-1)^n$$

Tenemos $\sqrt{d} = [a_1, a_2 \ldots, a_n, \alpha]$. Resolviendo esta ecuación para encontrar α, tenemos por tanto

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

Esto nos da que $(p_n - q_n\sqrt{d})\alpha = -(p_{n-1} - q_{n-1}\sqrt{d})$, multiplicando por $p_n + q_n\sqrt{d}$, tenemos

$$\alpha = (-1)^{n+1}(p_{-1} - q_{n-1}\sqrt{d})(p_n + q_n\sqrt{d})$$

Usando el hecho de que $p_nq_{n-1} - q_np_{n-1} = (-1)^n$, tenemos

$$\alpha = c + \sqrt{d}, \quad \text{donde} \quad c = (-1)^n(p_np_{n-1} - q_nq_{n-1}d)$$

En particular, esto nos dice que la fracción continua de $\sqrt{d}$ es periódica:

$$\sqrt{d} = [a_1, \ldots, a_n, c + \sqrt{d}] = [a_1, \overline{a_2, \ldots, a_n, c + a_1}]$$

Recíprocamente, asumimos que $\sqrt{d} = [a_1, \overline{a_2, \ldots, a_n, c + a_1}]$ para algún entero c, probaremos que $N(p_n + q_n\sqrt{d}) = (-1)^n$ y $c = a_1$. Nuestra hipótesis implica que $\sqrt{d} = [a_1, \ldots, a_n, c + \sqrt{d}]$, y por lo tanto

$$\sqrt{d} = \frac{(c + \sqrt{d})p_n + p_{n-1}}{(c + \sqrt{d})q_n + q_{n-1}}$$

Expresaremos el lado derecho como $x + y\sqrt{d}$ y comparamos coeficientes, multiplicando el numerador y denominador por $(c - \sqrt{d})q_n + q_{n-1}$, de manera que

$$\sqrt{d} = \frac{(cp_n + \sqrt{d}p_n + p_{n-1})(cq_n - \sqrt{d}q_n + q_{n-1})}{N}.$$

donde $N = N(cq_n + q_{n-1} + \sqrt{d}q_n)$. Desarrollando y cancelando términos tenemos

$$\sqrt{d} = \frac{(cp_n + p_{n-1})(cq_n + q_{n-1}) - dp_nq_n + \sqrt{d}(p_nq_{n-1} - q_np_{n-1})}{N}.$$

Por último comparamos coeficientes, tenemos que $N = p_nq_{n-1} - q_np_{n-1} = (-1)^n$. Por el teorema anterior tenemos que $\frac{cq_n + q_{n-1}}{q_n}$ es un convergente de la fracción continua de $\sqrt{d}$ y por tanto $cq_n + q_{n-1} = p_n$. En particular, $N = N(p_n + q_n\sqrt{d}) = (-1)^n$.

La ecuación $cq_n + q_{n-1} = p_n$, implica que $c = \frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}}$, y tenemos

$$\frac{p_n}{q_n} - 1 < c < \frac{p_n}{q_n}.$$

Ya que $\lfloor\sqrt{d}\rfloor \leq \frac{p_n}{q_n} \leq \lfloor\sqrt{d}\rfloor + 1$, por tanto:

$$\lfloor\sqrt{d}\rfloor - 1 < c < \lfloor\sqrt{d}\rfloor + 1.$$

Como c es un entero, tenemos $c = \lfloor\sqrt{d}\rfloor = a_1$. Por lo tanto,

$$\sqrt{d} = [a_1, \overline{a_2, \ldots, a_n, 2a_0}].$$

□

Observación 6. Observemos que si tenemos una fracción continua periódica

$$[a_1, \ldots, a_n, \overline{a_{n+1}, \ldots, a_{n+m}}]$$

también la podemos escribir como

$$[a_1, \ldots, a_n, \overline{a_{n+1}, \ldots, a_{n+m}, a_{n+m+1}, \ldots, a_{n+km}}] \ ,$$

de manera que la longitud del periodo (en esta última expresión) es mk para un entero $k > 0$ cualquiera. Evidentemente, existe un m mínimo de manera que la longitud del periodo es m.

El Teorema 18 nos asegura que cualquir solución (x, y) de la ecuación de Pell $x^2 - dy^2 = \pm 1$ se obtiene a partir de un convergente de la fracción continua de $\sqrt{d}$, $\sqrt{d} = [a_1, \ldots, a_m, \ldots]$, es decir, $x/y = p_m/q_m$ para algún m. Además, el Teorema 19 nos garantiza que en ese caso se tiene que $\sqrt{d} = [a_1, \overline{a_2, \ldots, a_m, 2a_1}]$. Por lo tanto m es un múltiplo de la longitud mínima del periodo de $\sqrt{d}$. Estos resultados, junto con el Teorema 16 (alternativamente, el Teorema 19 también se podría utilizar en este sentido) nos permiten asegurar:

Corolario 4. *Sea $\sqrt{d} = [a_1, \overline{a_2, \ldots, a_n, 2a_1}]$ con n mínimo la fracción continua periódica de $\sqrt{d}$. Entonces $p_n^2 - q_n^2 d = (-1)^n$ y en consecuencia, si n es par $\epsilon = p_n + q_n\sqrt{d}$ es la unidad fundamental de $\mathbb{Z}[\sqrt{d}]$ y si n es impar lo es $\epsilon = p_{2n} + q_{2n}\sqrt{d}$.*

Los resultados anteriores completan el cálculo de las unidades del anillo $\mathbb{Z}[\sqrt{d}]$, no obstante sabemos que si $d \equiv 1 \mod 4$ el anillo de enteros de $\mathbb{Q}(\sqrt{d})$ es $\mathbb{Z}[\alpha$, con $\alpha = (1 + \sqrt{\alpha})/2$. El resultado siguiente completa el cálculo de las unidades en este caso y finaliza el problema que nos planteábamos.

Proposición 12. *Sea $d \equiv 1 \mod 4$ libre de cuadrados, $d > 1$ y $\alpha = (1 + \sqrt{d})/2$. Sea $x - y\alpha \in (-1, 1)$ una unidad en $\mathbb{Z}[\alpha]$ con $y > 0$. Entonces, $\frac{x}{y}$ es un convergente de expresión de α como una fracción continua.*

Demostración. Sea $A = x - y\alpha$. Como $|A| < 1$, se tiene que $x > y\alpha - 1$ y en particular x es positivo. Como A es una unidad, tenemos que $|x - y\alpha| \cdot |x - y\overline{\alpha}| = 1$.

Por lo tanto,

$$\left|\frac{x}{y} - \alpha\right| = \frac{1}{|y| \cdot |x - y\overline{\alpha}|}.$$

Como $x > y\alpha - 1$, tenemos que $x - y\overline{\alpha} > \delta y - 1$ donde $\delta = \alpha - \overline{\alpha}$. El número δ es $\sqrt{d}$ o $2\sqrt{d}$, dependiendo de si d es o no congruente con 1 módulo 4.

Supongamos ahora que $y > \frac{1}{\delta - 2}$. Esto implica que $\delta y - 1 > 2y$, y por lo tanto

$$\left|\frac{x}{y} - \alpha\right| < \frac{1}{2y^2}$$

Esto nos dice que $\frac{x}{y}$ es un convergente de α.

Esto lleva a considerar los casos donde $1 \leq y \leq \frac{1}{2\sqrt{2} - 2}$. En particular, nosotros tenemos $\delta < 3$, que solamente ocurre en los casos $d = 2$ o $d = 5$. En el caso $d = 2$, la desigualdad $1 \leq y \leq \frac{1}{2\sqrt{2} - 2}$ implica $y = 1$. Ya que $A = x - \sqrt{2}$ es una unidad, podemos ver facilmente que $x = 1$. El resultado es cierto en este caso porque $\frac{1}{1}$ es un convergente de $\sqrt{2}$. En el caso $d = 5$, la desigualdad $1 \leq y < \frac{1}{\sqrt{5} - 2}$ implica que $1 \leq y < 5$. Hay cuatro unidades A satisfaciendo las condiciones:

$$1 - \alpha, 2 - \alpha, 3 - 2\alpha, 5 - 3\alpha.$$

Debemos comprobar todas las fracciones $\frac{1}{1}, \frac{2}{1}, \frac{3}{2}$ y $\frac{5}{3}$ son convergentes de $\frac{1+\sqrt{5}}{2}$. Más aún, la expresión de $\frac{1+\sqrt{5}}{2}$ como una fracción continua es $[1, 1, \ldots]$, y los convergentes son los ratios de los sucesivos números de Fibonacci.

□

Bibliografía

[1] F. Delgado, C. Fuertes, S. Xambó. Intorducción al Álgebra Vol II: Anillo, Factorización y Teoría de Cuerpos. Publicaciones de la Universidad de Valladolid. 350pp. 1998. ISBN: 84-7762-866-1

[2] G.H. Hardy and E.M. Wrigth. Introduction to the Theory of Numbers. Oxford University Press. Fifth edition. 1979.

[3] Richard Michael Hill. Introduction to number theory. Essential Textbooks in Mathematics. World Scientific. 2018

[4] William J. LeVeque. Fundamentals of Number Theory. Dover. 1977.

[5] C. D. Olds. Cntinued Fractions. Random House. 1963.

[6] A. Baker. Breve introducción a la teoría de números. Alianza Universidad. 1986.

[7] A.Baker. Transcendental Number Theory. Cambridge University Press. 1975.

[8] D.A.Cox. Primes of the Form x^2+ny_2:Fermat, Class Field Theory, and Complex Multiplication. Wiley. 2013.

[9] I. Stewart and D.Tall. Algebraic Number Theory and Fermat's Last Theorem. Chapman and Hall. 2015.