USC UNIVERSIDADE DE SANTIAGO DE COMPOSTELA
FACULTADE DE MATEMÁTICAS

Traballo Fin de Grao

Fracciones continuas: ecuación de Pell-Fermat

Yeray García Gómez

07, 2022

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

GRAO DE MATEMÁTICAS

Traballo Fin de Grao

Fracciones continuas: ecuación de Pell-Fermat

Yeray García Gómez

07, 2022

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Trabajo propuesto

Área de Coñecemento: Álxebra
Título: Fracciones continuas: ecuación de Pell-Fermat
Breve descrición do contido
Se desarrollará el algoritmo de las fracciones continuas. Se aplicará a la discusión y resolución y de la ecuación de Pell-Fermat.
Recomendacións
Aparicio, E.Teoría de los números, Univ País Vasco 1993 Baker, A. Theory of numbers, Cambridge 1984 Leveque, W. Fundamentals of number theory, Addison-Wesley 1977
Outras observacións

Índice

Resumen

En esta memoria se aborda en un primer momento una serie de propiedades de la representación de los números en su forma de fracción continua de una manera general, para luego ver la representación de las Irracionalidades Cuadráticas que se usaran en la siguiente sección, esta representación de las Irracionalidades Cuadraticas fue utilizada, gracias a su increíble forma que se ve a lo largo de esta sección, para demostrar la irracionalidad de, por ejemplo, el numero e y de π . En cuanto a la segunda sección, la cual es el centro de este trabajo, aborda la Ecuación de Pell, un caso especial de representación por formas cuadráticas binarias, y su resolución efectiva, todo gracias al célebre teorema de las unidades de Dirichlet, haciendo uso de esta estructura de las unidades de los cuerpos cuadráticos reales y el algoritmo de las fracciones continuas para Irracionalidades Cuadráticas que antes ya hemos introducido, usando que la Ecuación de Pell involucra una Irracionalidad Cuadrática. En el ultimo apartado de esta segunda sección se abordara una pequeña generalización a formas binarias introduciendo la Clase de Pell y su posible resolución utilizando propiedades antes mencionadas de la Ecuación de Pell.

Abstract

In this statement it will deal in first place a series of properties of the representation of numbers in their expresion in continued fraction in a general way, to see then the representation of the Quadratic Irrationalities thath we will use them in the next section, this representation of the Quadratic Irrationalities was used, thanks of their great properties that is exposed throughout this first section, to see the irrationalitie of, for example, e and π. As regard of the second section, which is the central section in this assignment, present the Pell's Ecuation, a special kind of the representation of numbers by binaries quadratic form, and its efective resolution, all of this thanks to the celebrated Dirichlet's unities Theorem, making use of the structure of the real quadratic field's unities and the algorithm of the continued fraction for Quadratic Irrationalities that we

introduced, using that Pell's Ecuation involve a Quadratic Irrationalitie. Lastly in the final part of this section we present a generalization of binay forms intoducing the Pell's Class and its possible resolution using the properties of Pell's ecuation.

Introducción

En esta memoria se pretende abordar una de las aplicaciones del célebre teorema de las unidades de Dirichlet, de un cuerpo global(números algebraicos y funciones algebraicas). Realmente aquí vamos a considerar un caso muy particular: La estructura de las unidades de un cuerpo cuadrático real. Para una demostración moderna de aquel teorema de Dirichlet recomendamos al lector a [4], [6] y [8]. Como se puede apreciar en estas referencias este teorema está fuera de una materia de grado, y en aplicaciones importantes están en la llamada Teoría de Cuerpos de Clases (TCC).

La aplicación antes mencionada es la llamada ecuación de Pell-Fermat, cuya discusión y resolución efectiva involucran a la estructura de las unidades de los cuerpos cuadráticos reales y al algoritmo de las fracciones continuas.

La ecuación de Pell es un caso muy especial de representación pr formas cuadraticas binarias. Esta representación da lugar a na teoría avanzada dentro de la Teoría de Números: el teorema del genero, cuyo teorema de existencia es esencialmente equivalente a otro célebre de Dirichlet, el de densidad de números primos den progresiones aritméticas.

La expresión en fracciones continuas de los números reales está relacionada con problemas importantes en Teoría de Números. En 1737 Euler las utilizó para probar la irracionabilidad de e, y más adelante Lambert para probar la de π (Conjetura de la Grecia helénica resuelta). En efecto, a diferencia de la expresión decimal, que depende de la base del sistema de numeración la expresión en fracciones continuas de un número real es absoluta. Y sobre todo, también a diferencia de aquella "discrimina los números racionales por tener expansiones finitas".

Mostraremos la eficacia del algoritmo de fracciones continuas para la ecuación de Pell, en relación a los algoritmos directos.

En este trabajo se mostraran de forma básica, los métodos del Álgebra en aritmética clásica: teoría de grupos y de extensiones de cuerpos, y de Teoría de Números Algebraica elemental (unidades de los cuerpos cuadráticos reales), son eficaces y organizan mejor los procedimientos más antiguos. Asimismo se muestran también los métodos analíticos, para fracciones continuas

y su aplicación de Pell.

Capítulo 1

Fracciones Continuas

Se han consultado las referencias [1], [2] y [5].

1.1. Propiedades

Tomamos un $\theta \in \mathbb{R}$, entonces denotemos $\theta_0 = \theta$, y $a_0 = [\theta_0]$. Si $a_0 = \theta_0$, entonces $\theta = a_0 \in \mathbb{Z}$, y si $a_0 \neq \theta_0$ y entonces podemos expresar $\theta = \theta_0 = a_0 + 1/\theta_1$ con $\theta_1 = \dfrac{1}{\theta_0 - a_0} > 1$, y $a_1 = [\theta_1]$, si $a_1 \neq \theta_1$, $\theta_1 = a_1 + 1/\theta_2$ con $\theta_2 = \dfrac{1}{\theta_1 - a_1} > 1$, $a_2 = [\theta_2]$ y $\theta_0 = a_0 + \dfrac{1}{a_1 + \dfrac{1}{\theta_2}}$. De este modo, para $\theta \in \mathbb{R}$, y habiendo concretado $\theta_0 = \theta$ podemos definir:

Definición 1.1. El cociente completo

$$\theta_n := \frac{1}{\theta_{n-1} - a_{n-1}} \tag{1.1}$$

Definición 1.2. El cociente parcial

$$a_n := [\theta_n] \tag{1.2}$$

Con $n = 1, \ldots, N$ con $N = min\{n \mid \theta_n - a_n = 0\}$

Denotemos:

$$\theta = [a_0; a_1, \ldots, \theta_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{\theta_n}}} \tag{1.3}$$

Proposición 1.3. *Este proceso termina, es decir, la fracción continua es finita si y solo si* $\theta \in \mathbb{Q}$.

Demostración. Si $\theta = \dfrac{a}{b} \in \mathbb{Q}$, entonces el algoritmo de Euclides del cálculo del mínimo común divisor proporciona una sucesión de cocientes:

	c	c_1	$\ldots$	c_n
a	b	r_1	$\ldots$	r_m
	r_1	r_2	$\ldots$	0

Así $\theta = \dfrac{a}{b} = [c; c_1, \ldots, c_n]$. El reciproco se verifica inmediatamente. □

Y en general:

$$\exists N = 1, \ldots, \infty \text{ tal que la sucesión } a_0, a_1, \ldots, a_n, \ldots \in \mathbb{Z} \begin{cases} a_n \geq 1 & \text{si} \quad 1 \leq n < N \\ a_n \geq 2 & \text{si} \quad n = N \\ a_n = 0 & \text{si} \quad n > N \end{cases}$$

correspondiente a nuestra fracción continua y entonces denotaremos de la siguiente forma:

$$[a_0; a_1, \ldots, a_n] \coloneqq a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}} \tag{1.4}$$

o también

$$\theta = [a_0; a_1, \ldots, a_{n-1}, \theta_n] \quad n > 0 \tag{1.5}$$

de esta manera a cada $\theta \in \mathbb{R}$ le corresponden una sucesión de fracciones:

Definición 1.4.

$$\frac{p_n}{q_n} \coloneqq [a_0; a_1, \ldots, a_n] \quad n \geq 0 \tag{1.6}$$

Las cuales denominaremos convergentes (o fracciones reducidas) del número real θ cuya fracción continua es $[a_0; a_1 \ldots, a_n, \ldots]$.

Entonces tenemos(introduciendo los términos -2 y -1):

$$\begin{array}{llll} p_{-2} = 0 & p_{-1} = 1 & p_0 = a_0 & p_n = p_{n-1}a_n + p_{n-2} \\ q_{-2} = 1 & q_{-1} = 0 & q_0 = 1 & q_n = q_{n-1}a_n + q_{n-2} \end{array} \tag{1.7}$$

y de la misma forma como podemos denotar $\theta = [a_0; a_1, \ldots, a_{n-1}, \theta_n] = \dfrac{\pi_n}{q_n}$

$$\left.\begin{array}{r} q_n\theta = \pi_n = p_{n-1}\theta_n + p_{n-2} \\ q_n = q_{n-1}\theta_n + q_{n-2} \end{array}\right\} \theta = \frac{p_{n-1}\theta_n + p_{n-2}}{q_{n-1}\theta_n + q_{n-2}} \tag{1.8}$$

Proposición 1.5. *Se cumple que:*

$$\left.\begin{array}{l} p_n q_{n-1} - p_{n-1} q_n = (-1)^{n+1} \\ p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n \end{array}\right\} \quad \forall n \in \mathbb{N} \tag{1.9}$$

Demostración. Se obtiene recurrente mente aplicando las formulas de 1.7.

□

Corolario 1.6. *Se tiene que* $(p_n, q_n) = 1$, $\forall n$ *es decir el numerador y denominador de un convergente son primos entre sí*

Demostración. Se sigue de la formula 1.9.

□

Corolario 1.7. *Se verifican las igualdades:*

$$\left.\begin{array}{l} \dfrac{p_{n+1}}{q_{n+1}} - \dfrac{p_n}{q_n} = \dfrac{(-1)^{n+1}}{q_{n+1} q_n} \\ \dfrac{p_{n+1}}{q_{n+1}} - \dfrac{p_{n-1}}{q_{n-1}} = \dfrac{(-1)^{n+1} a_n}{q_{n+1} q_n} \end{array}\right\} \tag{1.10}$$

Demostración. También se sigue de 1.9. □

Proposición 1.8. *Las sucesiones de los numeradores y denominadores de los convergentes:*

$$q_{-1}, q_0, q_1, q_2, \ldots \tag{1.11}$$

$$p_{-2}, p_{-1}, p_0, p_1, p_2, \ldots \tag{1.12}$$

son estrictamente crecientes (si $a_0 \geq 0$ *)*

Demostración. Se sigue de la formula 1.7. □

Proposición 1.9. *En la situación de 1.4 se tiene que la sucesión de convergentes:* $\{\dfrac{p_n}{q_n}\}$ *es de Cauchy.*

Demostración. Entonces en la situación de 1.4 de la primera igualdad de 1.10 se tiene $\frac{p_{2k}}{q_{2k}} < \frac{p_{2k+1}}{q_{2k+1}}$. Por tanto ambas sucesiones tienen el mismo límite, de nuevo por la primera igualdad de 1.10. □

Proposición 1.10. *En la situación de* (1.1) *se tiene*

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} \leq \ldots < \theta < \ldots < \frac{p_5}{q_5} < \frac{p_3}{q_3} < \frac{p_1}{q_1}$$

Demostración. Gracias a 1.10 tenemos:

$$\frac{p_{2n}}{q_{2n}} < \frac{p_{2n+1}}{q_{2n+1}}$$

Y deduciendo de $a_n \leq \theta_n$ en:

$$\frac{p_n}{q_n} = [a_0; a_1, \ldots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}$$

$$\theta = [a_0; a_1, \ldots, \theta_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{\theta_n}}}$$

entonces $\frac{p_n}{q_n} < \theta$ si n par, $\frac{p_n}{q_n} > \theta$ si n impar. □

Proposición 1.11.

$$\frac{1}{q_k(q_n - 1_{n+1})} < \left|\theta - \frac{p_n}{q_n}\right| < \frac{1}{q_n - q_{n+1}} < \frac{1}{q_n^2} \tag{1.13}$$

Gracias a esta proposición tenemos el siguiente teorema:

Teorema 1.12. *La sucesión de convergentes del numero θ en efecto converge a θ:*

$$\frac{p_n}{q_n} \to \theta$$

Teorema 1.13. *El Teorema anterior y la construcción* (1.4) *determina una biyección entre $\mathbb{R}$ y la sucesión:*

$$a_0, a_1, \ldots, a_n, \ldots$$

con $a_n \geq 1$ si $n \geq 1$ o mejor dicho $\exists N \in \mathbb{N} \cup \infty$ tal que:

$$\begin{cases} a_n = 0 & n > N \\ a_n \geq 2 & n = N \\ a_n \geq 1 & n = 1, \ldots, N-1 \end{cases}$$

Demostración. La Existencia es inmediato.

Entonces hay que ver la unicidad:

La aplicación: $a = a_0, a_1 \ldots \rightarrowtail [a_0; a_1 \ldots]$ es inyectiva.

En efecto; sea:

$$\theta = [a_0; a_1, \ldots,] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots}},$$

con $0 < \theta - a_0 < 1$. Luego $a_0 = [\theta]$.

Sea $\theta_1 = \dfrac{1}{\theta - a_0} = a_1 + \dfrac{1}{a_2 + \ldots}$. Así $0 < \theta_1 - a_1 < 1$. Luego $a_1 = [\theta_1]$.

Procediendo de manera similar para los consecutivos a_n obtendríamos el resultado.

□

Proposición 1.14. *De dos convegentes a θ consecutivos al menos uno verifica:*

$$\left|\theta - \frac{p}{q}\right| < \frac{1}{2q^2}$$

Demostración. Ya que $\theta - \dfrac{p_n}{q_n}$, $\theta - \dfrac{p_{n+1}}{q_{n+1}}$ tienen signos opuestos:

$$\begin{aligned}\left|\theta - \frac{p_n}{q_n}\right| + \left|\theta - \frac{p_{n+1}}{q_{n+1}}\right| = \\ = \left|\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}}\right| = \\ = \frac{1}{q_n q_{n+1}} < \\ < \frac{1}{2q_n^2} + \frac{1}{2q_{n+1}^2} (Comode : \\ (a^2 + b^2) = a^2 + b^2 + 2ab)\end{aligned}$$

□

Proposición 1.15. *La distancia de los sucesivos convergentes de θ y el número θ, es decir $\left|\theta - \dfrac{p_n}{q_n}\right|$ es estrictamente decreciente.*

Demostración. Por 1.8:

$$q_n\theta - p_n = \frac{q_n p_n \theta_{n+1} + q_n p_{n-1}}{q_n\theta_{n+1} + q_{n-1}} - p_n = \frac{(-1)^2}{q_n\theta_{n+1} + q_{n+1}}$$

Pero:

$$q_{n-1}\theta_n + 1_{n-2} < q_{n-1}(a_n + 1) + q_{n-2} = \tag{1.14}$$

$$= 1_n + q_{n-1} < q_n\theta_{n+1} + q_{n-1}, \quad n \geq 1. \tag{1.15}$$

Entonces tenemos el resultado. □

Teorema 1.16. *Sea* $\frac{p}{q}$ *con* $0 < q < q_{n+1}$ *se tiene que:*

$$\left|q\theta - p\right| \geq \left|q_n\theta - p_n\right|$$

Demostración. Sea $u, v \in \mathbb{Z}$, tales que

$$\left.\begin{aligned} p &= up_n + vp_{n+1} \\ q &= uq_n + vq_{n+1} \end{aligned}\right\} \tag{1.16}$$

$$(det = (-1)^{n+1}) : \begin{pmatrix} p_n & p_{n+1} \\ q_n & q_{n+1} \end{pmatrix} \in Gl\,(2, \mathbb{Z}) \tag{1.17}$$

Si $u = 0$:

$$\frac{p}{q} = \frac{p_{n+1}}{q_{n+1}}$$

Pero $\frac{p_{n+1}}{q_{n+1}}$ es irreducible. Luego $u \neq 0$ y además si $v \neq 0$, entonces u, v tienen signos opuestos. Como también $q_n\theta - p_n,\ q_{n+1}\theta - p_{n+1}$ tienen signos opuesto. Luego:

$$\begin{aligned} |q\theta - p| =& |u(q_n\theta - p_n) + v(q_{n+1}\theta - p_{n+1})| = \\ =& |u(q_n\theta - p_n)| + |v(q_{n+1}\theta - p_{n+1})| \leq \\ \leq& |q_n\theta - p_n|. \end{aligned}$$

□

Teorema 1.17. *Sea* $\frac{p}{q} \neq \frac{p_n}{q_n}$, *con* $0 < q \leq q_n$ *se verifica:*

$$\left|q\theta - p\right| \geq \left|q_n\theta - p_n\right|$$

Demostración. En otro caso tendriamos:

$$\left|\theta - \frac{p_{n-1}}{q_{n-1}}\right| > \left|\theta - \frac{p_n}{q_n}\right| \geq \left|\theta - \frac{p}{q}\right|$$

Así, puesto que θ está entre $\frac{p_{n-1}}{q_{n-1}}$ y $\frac{p_n}{q_n}$, también está $\frac{p}{q}$, por lo cual:

$$\left|\frac{p}{q} - \frac{p_{n-1}}{q_{n-1}}\right| < \left|\frac{p_{n-1}}{q_{n-1}} - \frac{p_n}{q_n}\right| = \frac{1}{q_{n-1}q_n}$$

Gracias al corolario 1.10.

Por lo tanto:

$$\frac{pq_{n-1} - qp_{n-1}}{qq_{n-1}} < \frac{1}{q_{n-1}q_n}$$

Pero $|pq_{n-1} - qp_{n-1}| \geq 1$ ya que si $\frac{p}{q} = \frac{p_{n-1}}{q_{n-1}}$ Tendríamos la 1ª igualdad de la demostración. Por tanto $q > q_n$. □

Definición 1.18. Se dice que $\frac{p}{q}$ es una mejor aproximación de un número $\theta \in \mathbb{R}$ si:

$$\forall\ \frac{p'}{q'} \neq \frac{p}{q}$$

Entonces:

$$|q\theta - p| < |q'\theta - p'|$$

Observación 1.19. Si $\theta \notin \mathbb{Q}$ es suficiente con $|q\theta - p \leq |q'\theta - p$ y así el Teorema 1.16 implica el Teorema 1.17.

Esta definición de mejores aproximaciones nos lleva a conosiderar:

Definición 1.20. Una sucesión de fracciones $\left\{\frac{p_n}{q_n}\right\}_{n\geq 0}$ se dicen que es una sucesión de mejores aproximaciones si:

$$\left\{\frac{p_n}{q_n}\right\} \to \theta \quad \text{y} \quad \nexists \frac{p'}{q'} \neq \frac{p_n}{q_n}\ ,\ q_n \leq q' < q_{n+1} \quad \text{tal que}$$

$$|q_n\theta - p| < |q_n\theta - p_n|$$

Ejemplo 1.21. Tomando $\theta = \pi$. Si consideramos la aproximación decimal:

$$\theta = \sum_{n=-N}^{+\infty} \frac{a_n}{b^n},\ 0 \leq a_n < b,$$

en el caso de π ($b = 10$), obsevado los primeros 'convergentes' decimales:

$$\pi \approx 3,1415926\ldots$$

, éstos serán:

$$r_0 = \frac{3}{1},\ r_1 = \frac{31}{10},\ r_2 = \frac{314}{100} = \frac{157}{50},\ r_3 = \frac{3141}{1000}$$

Pero no son las mejores aproximaciones; sino que lo van a ser los convergentes a π, que gracias a su aproximación a en forma de fracción continua:

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

Y por tanto son las siguientes:

$$\delta_0 = \frac{3}{1} \qquad \delta_1 = 3 + \frac{1}{7} = \frac{22}{6}$$
$$\delta_2 = 3 + \frac{1}{7 + \frac{1}{15}} = \frac{333}{104} \quad \delta_3 = 3 + \frac{1}{7 + \frac{1}{16}} = \frac{355}{113}$$

Por tanto por los teoremas anteriores nos aseguran que los convergentes son parte de estas mejores aproximaciones, ahora bien, nos podemos preguntar si son las únicas, la respuesta es si, pero antes de probarlo veamos un teorema:

Teorema 1.22. *(Dirichlet)*

Sea $\theta \in \mathbb{R},\ \forall \tau \in \mathbb{R}^+$ *Entonces:*

$$\exists \frac{p}{q},\ 0 < q \leq \tau,\ |q\theta - p| < \frac{1}{\tau}$$

Demostración. Inmediato del principio de Dirichlet(del palomar). □

Corolario 1.23. $\theta \notin \mathbb{Q}$ *equivale a que la desigualdad:*

$$\left|\theta - \frac{p}{q}\right| < \frac{1}{q^2}$$

tiene ∞ *soluciones racionales para cada entero* $q > 0$

Observación 1.24. El Teorema 1.22 se puede deducir del Teorema 1.17, y el corolario 1.23 es parte de la proposición 1.10. Sin embargo usaremos el Teorema 1.22 para dar otra demostración del Teorema 1.16, en efecto: Así tomando $\theta \in \mathbb{R}$, $P_0 = [\theta]$,$Q_0 = 1$; $\frac{P_0}{Q_0}$ es mejor aproximación si $\theta - [\theta] \leq \frac{1}{2}$. De este modo si $Q_0\theta - P_0 \neq 0$, entonces sea Q_1 mínimo para $0 < Q_1 \leq \frac{1}{Q_0\theta - P_0},\ |Q_1\theta - P_1| < |Q_0\theta - P_0|$ Para algun P_1, del la misma forma razonamos con Q_2,$Q_3, \ldots$

Y por tanto para una sucesión $\frac{P_n}{Q_n}$, tenemos:

$$1 \leq Q_0 < Q_1 < \ldots \tag{1.18}$$

$$|Q_{n+1}\theta - P_{n+1}| < |Q_n\theta - P_n| \tag{1.19}$$

$$0 < q < Q_{n+1} \Rightarrow |Q_n\theta - P_n| < |q\theta - p|, n \leq 1 \tag{1.20}$$

$$|Q_n\theta - P_n| \leq \frac{1}{Q_{n+1}}, n \leq 1 \tag{1.21}$$

Entonces por estas relaciones y el teorema [] tenemos el siguiente teorema:

Teorema 1.25. *Los convergentes de θ son exactamente las mejores aproximaciones de θ.*

Demostración. $\Leftarrow$ Teorema 1.17.

$\Rightarrow$ Sea $\frac{p}{q}$ una mejor aproximación a θ. Entonces $q_n \leq q < q_{n+1}$. Entonces por el Teorema 1.16:

$$|q_n\theta - p_n| \leq |q\theta - p$$

Pero si $\frac{p_n}{q_n} \neq \frac{p}{q}$, entonces por ser mejor aproximación:

$$|q\theta - p| < |q_n\theta - p_n|$$

Lo cual supone una contradicción, teniendo asi la segunda inclusión.

□

Proposición 1.26. *Si*

$$\left|\theta - \frac{p}{q}\right| < \frac{1}{2q^2}$$

Entonces $\frac{p}{q}$ es convergente de θ.

Explicitamente, si $q_n \leq q < q_{n+1}$, entonces $\frac{p}{q} = \frac{p_n}{q_n}$.

Demostración. En cualquier caso necesitamos el Teorema 1.16.

$$\left|\frac{p}{q} - \frac{p_n}{q_n} \leq \left|\theta - \frac{p}{q}\right| + \left|\theta - \frac{p_n}{q_n} \leq (\frac{1}{q} + \frac{1}{q_n}|q\theta - p) < \frac{1}{qq_n}\right.\right.$$

Al ser $q_n \leq q$. Entonces:

$$|q_n p - p_n q| = 0$$

□

Definición 1.27. Se llama constante de Markov de θ $(M(\theta))$ al supremo del conjunto de $\lambda \in \mathbb{R}$ tal que la desigualdad:

$$\left|\theta - \frac{p}{q}\right| < \frac{1}{\lambda q^2}$$

tiene infinitas soluciones.

1.2. Irracionalidades Cuadraticas

Aunque el problema de calcular la mayor aproximación a θ esta resuelto con la expresión en fracción continua, salvo que θ sea de una forma muy concreta es imposible calcular la expresión concreta (como pasa con el caso de forma decimal). En general ni siquiera se tiene una regla de formación.

Sin embargo una aproximación en su forma decimal nos permite calcular términos de su expresión en fracción continua. Por ejemplo $2{,}7182 < e < 2{,}7183$ da:

$$e = [22; 1, 2, 1, 1, 4, 1, 1, \ldots]$$

Es conocido [Euler (1737)]:

$$2; 1, 2, 1, \ldots, 1, 2n, 1, \ldots$$

Probando así que $e \notin \mathbb{Q}$. Luego Lambert (1729-77) usó fracciones continuas para probar $\pi \notin \mathbb{Q}$

Para las irracionalidades cuadráticas existe un resultado completo, conocido desde la época de Lagrange y uno de los más notables resultados de teoría de números.

Teorema 1.28. *Los números reales que tienen una expresión periódica en fracción continua son exactamente los irracionales cuadráticos.*

Demostración. ($\Rightarrow$)

$$\theta = [a_0; a_1, a_2, \ldots, a_{k-1}, \overline{a_k, \ldots, a_{k+m-1}}]$$

$\theta_k = [\overline{a_k, \ldots, a_{k+m-1}}]$ verifica:

$$\theta_k = \frac{p'_{k-1}\theta_k + p_{k-2}}{q'_{k-2}\theta_k + q'_{k-2}}$$

Siendo $\frac{p'_m}{q'_m} \to \theta_n$. Y esta es una ecuación cuadrática.

Pero $\theta = \dfrac{p_{n-1}\theta_n + p_{n-2}}{q_{k-1}\theta_n + q_{n-2}}$ esto da una ecuación cuadrática para θ: si $a\theta_n^2 + b\theta_n + c = 0$, entonces, ya que:

$$\theta_n = -\frac{q}{den}$$

($\Leftarrow$) Sea $Irr\theta = ax^+bx + c,\ a, b, c \int \mathbb{Z}$ y $D = b^2 - 4ac > 0, \notin \dot{\mathbb{Q}}^2$.

(Así $\theta = \dfrac{-b + \sqrt{D}}{2} = \dfrac{-b + k\sqrt{d}}{2}$, $\mathcal{K} = \mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{d})$ d bien definido. $\theta' = \dfrac{-b - \sqrt{D}}{2}$ el conjugado de θ en $\mathcal{K}$.) Sea $f(x, y) = ax^2 + bxy + cy^2$ la clase de $D($ no necesariamente primitiva, aunque podriamos haber supuesto $(a\ b\ c) = 1)$ La sustitución:

$$x = p_n x' + p_{n-1}y'\ ,\ y = q_n x' + q_{n-1}y'$$

da:

$$f'_n(x,y) = a'_n x^2 + b'_n xy + c'_n y^2 \text{ en} D$$

$$\frac{a'_n}{q'_n} = \frac{1}{q_n^2} f(p_n, q_n) = f(\frac{p_n}{q_n}, 1) = f(\frac{p_n}{q_n}, 1) - f(\theta, 1) =$$
$$= a((\frac{p_n}{q_n})^2 - \theta^2) + b(\frac{p_n}{q_n} - \theta)$$

Pero $\left|\theta - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}$. Así:

$$\left|\theta^2 - (\frac{p_n}{q_n})^2\right| < \frac{\left|\theta - \frac{p_n}{q_n}\right|}{q_n^2} < \frac{2|\theta| + 1}{q_n^2}$$

Por lo tanto :

$$|a'_n| < (2|\theta| + 1)|a| + |b|$$

es decir, a'_n está acotado independientemente de n. Lo mismo para $c'_n = f(p_{n-1}, q_{n-1}) = a'_{n-1}$ y $b'_n (b'^2_n - 4a'_n c'_n = D)$. Pero $\theta = \dfrac{p_n \theta_{n+1} + p_{n-1}}{q_n \theta_{n+1} + q_{n-1}}$, por lo cual:

$$f_n(\theta_{n+1}, 1) = 0$$

ya que $f(\theta, 1) = 0$ Así θ_{n+1} es raíz de:

$$\left.\begin{aligned} a'^2_n x + b'_n x + a'_{n-1} &= 0 \\ b'^2_n - 4a'_n a'_{n-1} &= 0 \end{aligned}\right\} \tag{1.22}$$

Y al estar a'_n acotado por una constante fija solo hay un numero finito de valores para θ_n. En conclusión

$$\exists m \in \mathbb{N} \mid \theta_{k+m} = \theta_k$$

de donde se sigue la periodicidad.

□

Teorema 1.29. *Sea $\theta = [a_0; a_1, a_2, \ldots, a_n, \overline{a_{n+1}, \ldots, a_{n+m}}]$, esta expresión es puramente periódica $(n = 0)$ si y solo si θ es reducido $(\theta > 1, -1 < \theta' < 0)$*

Demostración. □

Teorema 1.30. *Si θ tiene su expresión en fracción continua puramente periódica entonces es de la forma:*

$$\theta = [a_0; \overline{a_1, a_2, \ldots, a_{n+m-1}, 2a_0}\ ]$$

Con $a_1, \ldots, a_{n+m-1}$ con simetría central, $m < 2\theta^2$, si y solo si $\theta = \sqrt{r}$, $r \in \mathbb{Q}_{>1} - \dot{\mathbb{Q}}$. Además si $r \in \mathbb{Z}$: $a_n < a_0$ $(n < m)$

Demostración. □

Ahora veamos un ejemplo:

Ejemplo 1.31. Tomemos $\theta = \sqrt{7}$: $\theta = [2; \overline{a_1, \ldots, a_m, 4}]$, $m < 14$, $an \leq 2$, $a1, \ldots, a_m$ simetria central:

$$\theta_0 = \sqrt{7} = 2 + (\sqrt{7} - 2), \qquad a_0 = 2 \tag{1.23}$$

$$,\theta_1 = \frac{1}{\theta_0 - a_0} = \frac{1}{\sqrt{7} - 2} = \frac{\sqrt{7} + 2}{3} = 1 + \frac{\sqrt{7} - 1}{3}, \qquad a_1 = 1 \tag{1.24}$$

$$,\theta_2 = \frac{3}{\sqrt{7} - 1} = \frac{\sqrt{7} + 1}{2} = 1 + \frac{\sqrt{7} - 1}{2}, \qquad a_2 = 1 \tag{1.25}$$

$$\theta_3 = \frac{2}{\sqrt{7} - 1} = \frac{\sqrt{7} + 1}{3} = 1 + \frac{\sqrt{7} - 1}{3}, \qquad a_3 = 1 \tag{1.26}$$

$$\theta_4 = \frac{3}{\sqrt{7} - 2} = \sqrt{7} + 2 = 4 + (\sqrt{7} - 2), \qquad a_4 = 4. \tag{1.27}$$

Por tanto: $\sqrt{7} = [2; \overline{1, 1, 1, 4}]$

A la vista de este ejemplo esto se puede organizar de la siguiente forma: Sea $d \in \mathbb{Z} - \mathbb{Q}^2$ y $\theta = \sqrt{d} = [a_0; a_1, \ldots, 2a_0]$ Tomemos:

$$b_0 = 0 \qquad ,b_n = a_{n-1}c_{n-1} - b_{n-1} \tag{1.28}$$

$$c_0 = 1 \qquad ,c_n = \frac{d - b_n^2}{c_{n-1}} \tag{1.29}$$

$$,a_n = [\frac{a_n + b_n}{c_n}], \quad n \leq 1 \tag{1.30}$$

$$\tag{1.31}$$

Por tanto: El periodo m es el mínimo común múltiplo de los periodos de b_n, c_n. Además, si

$$l = min\{b_{m+1} = b_m\}$$

$$n = min\{c_{m+1} = c_m\}$$

Si

$$l < n: \qquad m \text{ par y } l = \frac{m}{2} \tag{1.32}$$

$$n < l: \qquad m \text{ impar y } n = \frac{m-1}{2} \tag{1.33}$$

Si $d = p \equiv 1(4)$, primo, entonces m impar.

Este método proporciona un procedimiento efectivo del cálculo de la expresion $\theta = \sqrt{d}$, $d \in \mathbb{Z}^+ - \dot{\mathbb{Q}}^2$. Además permite cálculos simbólicos:

Ejemplo 1.32. $\theta = \sqrt{a^2-2},\ a \in \mathbb{Z}_{\geq 3}$. El desarrollo está claro y conduce a:

$$\sqrt{a^2-2} = [a-1; \overline{1, a-2, 1, 2a-2}]$$

.

Ejercicio 1.33. *1. Hallar los enteros $d > 0$ para los que $\sqrt{d} = [a; \overline{2a}]$. (Sol. $d = a^2+1$)*

2. Desarrollar la fracción continua de $\sqrt{a^2+1},\ a > 0$

Capítulo 2

La Ecuación de Pell-Fermat

Se han consultado las referencias [2], [3], [5] y [7].

2.1. Norma y Traza

Sea $f : V \to V$ un endomorfísmo de un k-espacio vectorial de dimensión n y los polinomios característico y mínimo $P_f(x)$ y $\mu_f(x) \in k[x]$. El teorema de Cayley-Hamilton, $P_f(f) = 0$, da $\mu_f(x)|P_f(x)$.

Se define la *traza* y la *norma* de f de la siguiente forma:

$$S_{V|k}(f) := \text{ coeficiente de } x^{n-1} \text{ en } P_f(x)5$$

$$N_{V|k}(f) := (-1)^n \text{ termino constante de } P_f(x) = det(f)$$

Sea ahora $K|k$ una extensión finita. Para $a \in K$ se tiene el endomorfismo $\alpha : K \to K$, el "producto por α", y así se definen las *aplicaciones traza* y *norma*:

$$S_{K|k}, N_{K|k} : K \to k$$

de la forma: $S_{K|k}(\alpha) := S_{K|k}$, $N_{K|k}(\alpha) := N_{K|k}(\alpha)$.

Proposición 2.1. *Sea $K|k$ una extensión finita. Se tiene que:*

i) $Irr(\alpha, k) = \mu_\alpha(x)$

ii) $P_a(x) = Irr(\alpha, k)^{K:k(\alpha)}$

iii) $S_{K|k}(\alpha) = [K : k]_i \sum \alpha^\sigma$ *y* $N_{K|k}(\alpha) = (\prod \alpha^\sigma)^{[K:k]}$, *donde σ recorre todos los encajes distintos $K \to \tilde{k}$ sobre k.*

Demostración. Efectivamente:

i) La composición $k[x] \to k(\alpha) \subset K \subset End_k(K)$ da la igualdad

ii) Se Cayley-Hamilton se sigue que $\mu_f(x)|P_f(x)$, y que tienen los mismos factores irreducibles.

iii) Se tiene que

$$S(\alpha) = \sum \text{raíces de } P_\alpha(x) = [K : k(\alpha)] \sum \text{raices de} Irr(\alpha, k) =$$
$$= [K : k(\alpha)][k(\alpha) : k]_i \sum \alpha^\sigma (\sigma : k(\alpha) \to \tilde{k} \text{ sobre } k) =$$
$$= [K : k]_i \sum \alpha^{sigma} (\sigma : k(\alpha) \to \tilde{k} \text{ sobre } k)$$

Analogamente para la norma

□

Proposición 2.2. *Sea $K|k$ una extensión finita. Entonces la norma $N : K \to k$ es un homomorfismo multiplicativo, y la traza $S : K \to k$ es un homomorfismo aditivo.*

Demostración. Inmediata de las definiciones ya que el determinante y la traza de un endomorfismo lo son, respectivamente, multiplicativo y aditivo. □

Proposición 2.3 (Fórmula de transitividad)**.** . *Para extensiones finitas $K|F|k$ se tiene*

$$N_{K|k} = N_{F|k} \circ N_{K|F} S_{K|k} = S_{F|k} \circ S_{K|F}$$

Demostración. Sea τ_j la familia de encajes distintos F en $\tilde{k}$ sobre k. Extendemos a cada τ_j a un encaje de K en $\tilde{k}$ y denotamos esta extensión también como τ_j. Sea σ_i la familia de encajes de K en $\tilde{k}$ sobre F(sin pérdida de generalidad se puede suponer que $K \subset \tilde{k}$). Si σ es un encaje de K en $\tilde{k}$ sobre k, para algún j, $\tau_j^{-1}\sigma$ deja invariable F, de donde $\tau_j^{-1}\sigma = \sigma_i$, para algún i. Luego $\sigma = \tau_j\sigma_i$ y, por consiguiente, la familia $\tau_j\sigma_i$ da todos los encajes distintos de K en $\tilde{k}$ sobre k. Como el grado de inseparabilidad es multiplicativo en las torres, es evidente la transitividad de la norma y de la traza. □

Proposición 2.4. *Si $K|k$ es finita separable, entonces la traza define una forma bilineal no singular:*

$$S : K \times K \to k, \ /x, y \mapsto S(xy)$$

Demostración. Si $0 = S(xK) = S(K)$, entonces $\sum \alpha^\sigma = 0$ por separabilidad. Esto no es posible por independencia lineal de caracteres. □

Si B es el anillo de enteros de un cuerpo de números algebraicos K, entonces la norma se extiende a los grupos (abelianos libres) de ideales(tratados en la parte de Álgebra Conmutativa de la materia de Álgebra Números y Geometría 21-22):

$$N_{\mathbb{Q}}^{K} : I(K) \to I(\mathbb{Q})$$

Proposición 2.5. *Sea I un ideal entero de K. Entonces:*

$$N_{\mathbb{Q}}^{K} = (B : I)\mathbb{Z}$$

Demostración. Sea $\mathfrak{p}|p$ primos de $B|\mathbb{Z}$.

Se tiene:

$$dim_{\mathbb{Z}/p\mathbb{Z}}(B/\mathfrak{p}) = f(\mathfrak{p}/p)$$

□

Proposición 2.6. *Sean $\overline{\mathbb{Z}}$ y $\overline{\mathbb{Q}}$ la clausura entera y algebraica de $\mathbb{Z}$ y $\mathbb{Q}$ en $\mathbb{C}$. Para los grupos de unidades se tiene:*

$$\mathcal{U}_{\overline{\mathbb{Z}}} = \overline{\mathbb{Z}} \cap N^{-1}\{\pm 1\}$$

denotando $N(\alpha) := N^{\mathbb{Q}(\alpha)_{\mathbb{Q}}(\alpha)}$ la norma absoluta de $\overline{\mathbb{Q}}$.

Demostración. Entonces:

"$\subset$" Si $\alpha \in \mathcal{U}_{\overline{\mathbb{Z}}}$, entonces $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha^{-1})$.

"$\supset$" Sea B el anillo de enteros de $\mathbb{Q}(\alpha)$. Se tiene entonces:

$$1 = |N(\alpha)| = (B : \alpha B)$$

por la proposición anterior

□

2.2. Ecuación de Pell y Estructura de las Unidades de Cuerpos Cuadráticos Reales

Las ecuaciones cuadráticas en 2 o más incógnitas tienen un grado dificultad elevado, por ejemplo de estas: La ecuación de Pell-Fermat, suma de dos, tres o mas cuadrados, representación de números por formas cuadráticas, $x^2+y^2 = z^2$,... Aunque existen algunos métodos generales,

como la teoría de Gauss sobre formas binarias, o el teorema de Hasse-Mikowski(para aplicación a sumas de varios cuadrados); comentaremos ilustrando el problema con la ecuación de Pell:

$$x^2 - dy^2 = 1 \tag{2.1}$$

con $d > 1$ libre de cuadrados. Es decir, analizaremos la representación del 1 por la forma cuadrática $f(x, y) = x^2 - dy^2$. El conjunto de soluciones es el núcleo de:

$$\begin{array}{ccc} \mathbb{Z}[\sqrt{d}] & & \\ \downarrow & \searrow^{N} & \\ \mathbb{Q}_n(\sqrt{d}) & \xrightarrow[N]{} & \mathbb{Q} \end{array}$$

Es decir $Sol(x^2 - dy^2 = 1) = Ker(N) \subset \mathcal{U}_{\mathbb{Z}[\sqrt{d}]}$, ya que $N(x + \sqrt{d}y) = x^2 - dy^2$.(Aclaración: denotamos $N = N_{|\mathbb{Z}[\sqrt{d}]}$). Gracias a que $N(-1) = (-1)^2 = 1$, si ε es solución, también lo es $\pm\varepsilon^{\pm 1}$, es decir tomando $\varepsilon = x + \sqrt{d}y$ como solución entonces $\pm(x \pm \sqrt{d}y)$ lo son. Y a su vez sabemos que si $\varepsilon = x + \sqrt{d}y$ es solución, entonces $|x| > -\sqrt{d}|y| > 0$. Por tanto trabajaremos con los siguientes conjuntos:

$$Ker(N)^+ = Ker(N) \cap \mathbb{R}^+ = Ker(N) \cap \{x + \sqrt{d}y,\ x > 1,\ y \neq 0\}$$

$$Ker(N)_{>1} = Ker(N) \cap \mathbb{R}_{>1} = Ker(N) \cap \{x + \sqrt{d}y,\ x > 1,\ y > 0\}$$

Siendo el primero un grupo y el segundo un semigrupo. Así por tanto como tenemos que

$$Ker(N) = \{\pm 1\} \times (Ker(N)_{>1})$$

$$Ker(N)^+ = Ker(N)_{>1} \sqcup \{1\} \sqcup (Ker(N)_{>1})^{-1}$$

Por tanto basta estudiar el semigrupo:

$$Ker(N)_{>1} = Ker(N) \cap \mathbb{R}_{>1}$$

Proposición 2.7. *Son equivalentes:*

i) La ecuación de Pell tiene solución no trivial$(\neq (\pm 1\ ,\ 0))$.

ii) $Ker(N)_{>1} \neq \emptyset$.

iii) $Ker(N)_{>1}$ *es infinito.*

Demostración. Obvia salvo $ii) \Rightarrow iii)$:

$\mathbb{R}^+$ es libre de torsión($\dot{\mathbb{R}} \times \mathbb{R}^+$, torsión $\times$ libre de torsión) $\square$

Esto fue conjeturado por Fermat, y fue Lagrange quien dio una demostración completa.

Ante todo afirmaremos más sobre los subgrupos de $\mathbb{R}$:

Proposición 2.8. *Cada subgrupo de $\mathbb{R}$ es discreto o denso.*

Demostración. Sea $\mathcal{H} \in \mathbb{R}$ y $0 < a < b$ tales que $(a, b) \cap \mathcal{H} = \emptyset$ por ser no denso.

Ahora supongamos que es no discreto.

Sean:

$$h \in \mathcal{H} \cap (0, \frac{b-a}{2})$$

$$n \text{ tal que } nh \leq a,\ (n+1)h > a$$

Así $(n+1)h \leq a + h < a + \dfrac{b-a}{2} < b$, es decir:

$$(n+1)h \in (a, b) \cap \mathcal{H}$$

Lo cual es es una contradicción, y por tanto tendríamos el resultado.

□

Proposición 2.9. *Para un subgrupo $\mathcal{H}$ de $\mathbb{R}$ son equivalentes:*

i) $\mathcal{H}$ *discreto.*

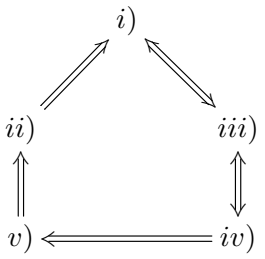
ii) $\mathcal{H}$ *cerrado propio.*

iii) $Inf\ \mathcal{H}^+ > 0$.

iv) $\exists min\ \mathcal{H}^+ > 0$.

v) $\mathcal{H}$ *cíclico infinito.*

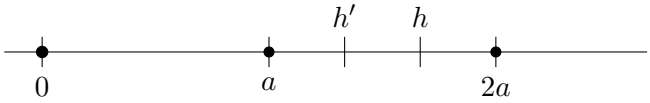
Demostración. Seguiremos el siguiente esquema de implicaciones:



ii)⇒i): Proposición anterior, ya que si es cerrado propio entonces no puede ser denso, por tanto solo queda que sea discreto.

i)⇔iii): i)⇔$\exists \mathcal{U} \ni 0, \mathcal{U} \cap \mathcal{H} = \{0\} \Leftrightarrow \exists \mathcal{U} \ni, \mathcal{U} \cap \mathcal{H}^+ = \emptyset \Leftrightarrow$iii)

iii)⇔iv) Tomando $a = Imf(\mathcal{H}^+)$.



Si $a \notin \mathcal{H}$, puesto que $a \in Cl(\mathcal{H})$, sean $h, h' \in \mathcal{H}$, $h' - a < h - a < a$. Asi $0 < h - h' < a$, lo cual supone una contradicción.

iv)⇒v): Sea $a = min\mathcal{H}^+$.

Para $h \in \mathcal{H}^+ \ \exists n, \ h \in [na, \ (n+1)a]$. Si $h \neq na$, entonces $0 < h - an < a$, lo cual es una contradicción por $h - an \in \mathcal{H}$. Por tanto $\mathcal{H} = a\mathbb{Z}$

v)⇒ii): Se tiene trivialmente.

□

Corolario 2.10. *Para $\mathcal{H}$ subgrupo de $\mathbb{R}^+$ son equivalentes:*

i) $\mathcal{H}$ *discreto.*

ii) $\mathcal{H}$ *cerrado propio.*

iii) $Inf \ \mathcal{H}^{>1} > 1$.

iv) $\exists min \ \mathcal{H}^{>1} > 0$.

v) $\mathcal{H}$ *cíclico infinito.*

Demostración. En este caso $\mathcal{H} = (min\mathcal{H}^{>}1)^{\mathbb{Z}}$ La función exponencial ($exp : \mathbb{R} \cong \mathbb{R}^+$) es un isomorfismo de grupos topológicos monótono. □

Aplicaremos esto para el cálculo de las unidades de los cuerpos cuadráticos reales. Tomemos $\mathcal{K} = \mathbb{Q}(\sqrt{d}) \subset \mathbb{R}$ por tanto:

$$\mathcal{U}_\mathcal{K} = \pm 1 \times \mathcal{U}_\mathcal{K}^+$$

y

$$\mathcal{U}_\mathcal{K}^{\geq 1} = \{x + \sqrt{d}y \in \mathcal{U}_\mathcal{K}, \ x, y > 0\}$$

Por tanto utilizando el corolario anterior podemos razonar que :

$\mathcal{U}_\mathcal{K}^+$ es cíclico infinito generado por $min \ \mathcal{U}_\mathcal{K}^{\geq 1} = x_0 + \sqrt{d}y_0$ siendo x_0, y_0 mínimos> 0 en $\mathcal{U}_\mathcal{K}$.

Definición 2.11. Al generador $x_0 + \sqrt{d}y_0$ se le denomina unidad fundamental de $\mathcal{K}$

Por lo tanto:

$$\mathcal{U}_{\mathcal{K}} = \{\pm 1\} \times (x_0 + y_0\sqrt{d})^{\mathbb{Z}} \cong \{\pm 1\} \times \mathbb{Z}$$

Se llega así al mismo resultado que el teorema de las unidades da, en este caso, ahora por procedimientos elementales.

Observación 2.12. En el caso de otros cuerpos de números algebraicos reales $\mathcal{K}$, el citado teorema de loas unidades da:

$$\mathcal{U}_{\mathcal{K}}^{+} \cong \mathbb{Z}^r$$

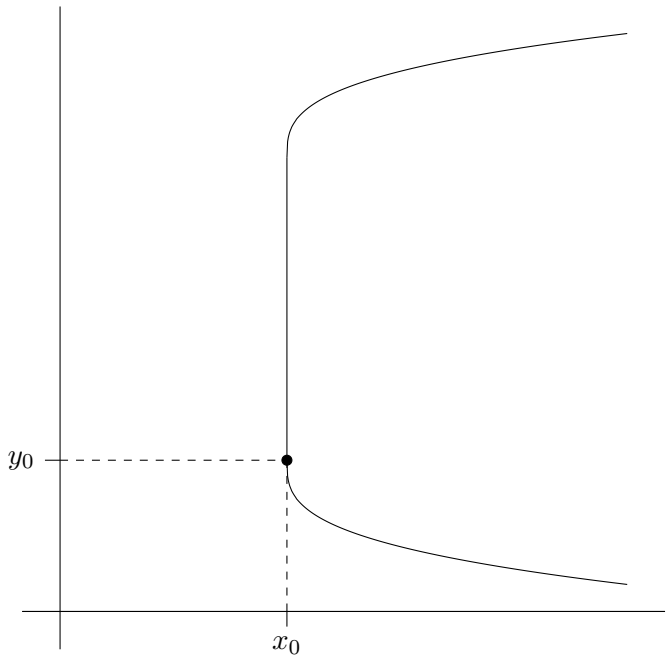
(r determinado por las unidades reales y complejas de $\mathcal{K}$). La discusión previa da :

$$r > 1 \Leftrightarrow \mathcal{U}_{\mathcal{K}} \text{ denso en } \mathbb{R}.$$

Realmente la igualdad :

$$Ker(N)^{>1} = Ker(N) \cap \{x + \sqrt{d}y,\ x > 1,\ y > 0$$

Prueba que su correspondiente en $\mathbb{Z}^2$ tiene proyecciones sobre los ejes, acotadas interiormente(por 1 y por 0). La existencia de mínimos de esta proyección, x_0, de la primera, e y_0, de la fibra de x_0, está garantizada si y solo si $Ker(N)^{>1} \neq \emptyset$.



Esto se puede deducir del algoritmo de fracciones continuas, como se ve a continuación, o bien del teorema de 1.22(Dirichlet).

2.3. Algoritmo de Fracciones Continuas y Ecuación de Pell

Teorema 2.13. *Se tiene que para un numero real $\theta \in \mathbb{R}$ y otro real positivo $\tau \in \mathbb{R}^+$ entonces:*

$$\exists \frac{p}{q},\ 0 < q \leq \tau,\ |q\theta - p| < \frac{1}{\tau}$$

Este teorema es necesario para probar que $\mathcal{U}_{\mathbb{Q}(\sqrt{d})} \supsetneq \{\pm 1\}$

Teniendo en cuenta el corolario 2.10 se tiene:

Lema 2.14. *Se tiene*

$$Inf(Ker(N)^{>}1) > 1$$

Demostración.

$$\{x + \sqrt{d}y \in \mathbb{Z}[\sqrt{d}],\ x > 1, y > 0\}$$

Está acotado por 3. □

Teorema 2.15. *Sea $d > 1$ libre de cuadrados. La ecuación de Pell $x^2 - dy^2 = 1$ tiene infinitas soluciones $KerN = \{\pm 1\} \times Ker(N)^+$.*

$$KerN^+ = min(KerN^{>1})^{\mathbb{Z}}(\textit{cíclico infinito}) = (x_0 + y_0 + \sqrt{d})^{\mathbb{Z}}$$

Siendo $x_0 + y_0\sqrt{d}$ la llamada solución fundamental. Ademas:

$$x_0 = min\{x \in \mathbb{Z}, \exists y, x + y\sqrt{d} \in KerN^{>1}\}$$

$$y_0 = min\{y \in \mathbb{Z}, \exists x, x + y\sqrt{d} \in KerN^{>1}\} = min\{y \in \mathbb{Z}, x_0 + y\sqrt{d} \in KerN^{>1}\}$$

Demostración. Por el lema 2.14 y del corolario 2.10 sobre las afirmaciones sobre los mínimos se sigue de:

$$x + \sqrt{d}y \in Ker(N)_{>1}:$$
$$(x + \sqrt{d}y)(x_0 + \sqrt{d}y_0) = x_1 + \sqrt{d}y_1 \ \Rightarrow$$
$$x1 > x,\ y_1 > y$$

□

El cálculo efectivo de este conjunto de soluciones $(Ker(N)^+)$ está relacionado con el algoritmo de las fracciones continuas de los irracionales cuadráticos(reales, en este caso).

Ante todo si $x+\sqrt{d}y \in Ker(N)_{>1}$ entonces $x > \sqrt{d}y$. Así $x+\sqrt{d}y > 2\sqrt{d}y$, de donde se deduce:

$$x-\sqrt{d}y = \frac{1}{x+\sqrt{d}y} < \frac{1}{2\sqrt{d}y}$$

En consecuencia $\frac{x}{y}-\sqrt{d} < \frac{1}{2y^2}$. De este modo tenemos que $\frac{x}{y}$ es un convergente a $\sqrt{d}$ por lo visto en 1.26. Ahora tenemos que averiguar qué convergentes a $\sqrt{d}$ son los elementos de $Ker(N)_{>1}$.

Sea $\sqrt{d} = [a_0; \overline{a_1, \ldots, a_m}]$

Sea $\frac{p_n}{q_n}$ $(n = 1, 2, \ldots)$ los convergentes a $\sqrt{d}$ y θ_n $(n = 0, 1, \ldots)$ los cocientes convergentes.

Teorema 2.16. *El numero $p_n + \sqrt{d}q_n \in Ker(N)_{>1}$ si y solo si:*

$$n = lm-1 \left| \begin{array}{l} l = 1,2,3,\ldots \quad si \quad m\ par \\ l = 2,4,6,\ldots \quad si \quad m\ impar \end{array} \right. \tag{2.2}$$

Sí y solo sí $2, m|(n+1)$

Demostración. $(\Rightarrow)$ Ante todo n debe ser impar, ya que para que $p_n + \sqrt{d}q_n \in Ker\mathbb{N}_{>1}$, se tiene que tener $\frac{x}{y} > \sqrt{d}$, y solo los convergentes impares son menores a $\sqrt{d}$. Por tanto basta probar que $m|(n+1)$: Puesto que,

$$\sqrt{} = \frac{p_n\theta_{n+1} + p_{n-q}}{q_n\theta_{n+1} + q_{n-1}}$$

se tiene que:

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

. Y gracias a que

$$p_n^2 - dq_n^2 = 1$$

Obtenemos:

$$\begin{aligned} \theta_{n+1} = (p_n^2 - dq_n^2)\theta_{n+1} = & \quad -(p_{n-1} - \sqrt{d}q_{n-1})(p_n + \sqrt{d}q_n) \\ = & \quad (-1)^{n-1}\sqrt{d} + c\ , c \in \mathbb{Z} \\ = & \quad \sqrt{d} + c\ , \text{ya que } n \text{ impar} \end{aligned}$$

Pero $\theta_{n+1} = a_{n+1} + \frac{1}{\theta_{n+2}} = a_0 + \frac{1}{\theta_1} + c$. Como $a_{n+1} = a_0 + c = [\theta_{n+1}]$, entonces $\frac{1}{\theta_{n+2}} = \frac{1}{\theta_1}$ la parte entera de θ_{n+1}. Es decir θ_{n+2}=θ_1. Puesto que el periodo es m se tiene :

$$m|(n+1)$$

($\Leftarrow$) Puesto que $m|(n+1)$ se tiene: $\theta_1 = \theta_{n+2}$ y así:

$$\sqrt{d} = \frac{p_{n+1}\theta_1 + p_n}{q_{n+1}\theta_1 + q_n} =$$

$$= \frac{\frac{p_{n+1}}{\sqrt{d}-a_0} + p_n}{\frac{q_{n+1}}{\sqrt{d}-a_0} + q_n} =$$

$$= \frac{p_{n+1+p_n(\sqrt{d}-a_0)}}{q_{n+1} + q_n(\sqrt{d}-a_0)}$$

Le sigue:

$$\left.\begin{array}{rcl} p_n & = & q_{n+1} - a_0 q_n \\ p_{n+1} - a_0 p_n & = & d q_n \end{array}\right\}$$

Eliminando en a_0:

$$p_n^2 - dq_n^2 = p_n q_{n+1} - p_{n+1} q_n = (-1)^{n+1}$$

Y como n es impar:

$$p_n^2 - dq_n^2 = p_n q_{n+1} - p_{n+1} q_n = 1$$

□

Aplicando un análisis similar a la ecuación:

$$x^2 - dy^2 = -1,\ 0 < d \notin \mathbb{Q}^2$$

Sea $\mathcal{K}$ un espacio de números,y la aplicación norma:

$$N : \mathcal{K} \to \mathbb{Q}$$
$$N(\varepsilon) = \varepsilon \cdot \prod_{\sigma \neq 1} \varepsilon^\sigma$$

Por tanto:

$$N(\varepsilon) = 1 \ \Rightarrow\ \varepsilon^{-1} = \prod_{\sigma \neq 1} \varepsilon^\sigma$$

Ahora consideremos $\mathcal{R}$ un subanillo de $\mathcal{K}$ que verifica:

$$\varepsilon \in \mathcal{R},\ N(\varepsilon) = 1 \Rightarrow \prod_{\sigma \neq 1} \epsilon^\sigma \in \mathcal{R}$$

Y de este modo se cumple que:

$$(N_{|\mathcal{R}})^{-1}\{\pm 1\} \subset \mathcal{U}_{\mathcal{R}}$$

Esta hipótesis se cumple en los casos:

a) $\mathcal{R}$ abierto de enteros de $\mathcal{K}$

b) $\mathcal{K}$ de Galois, $\mathcal{R}^\sigma = \mathcal{R}\ \forall\sigma$.

A su vez tenemos que si $\mathcal{R}$ está contenido en un anillo de enteros, entonces:

$$\mathcal{U}_\mathcal{R} \subset (N_{|\mathcal{R}})^{-1}\{\pm 1\}$$

En general, si $\mathcal{K} \subset \mathbb{R}$:

$$(N_{|\mathcal{R}})^{-1}\{\pm 1\} = \{\pm 1\} \times (N_{|\mathcal{R}})^{-1}\{\pm 1\}^+$$
$$\mathcal{U}_\mathcal{R} = \{\pm 1\} \times \mathcal{U}_\mathcal{R}^+$$

ya que la torsión de ambos es $\{\pm 1\}$.
Si $[\mathcal{K} : \mathbb{Q}]$ es par, entonces:

$$(N_{|\mathcal{R}})^{-1}(1) = \{\pm 1\} \times (N_{|\mathcal{R}})^{-1}\{\pm 1\}^+$$

ya que $N(-1) = (-1)^{[\mathcal{K}:\mathbb{Q}]} = 1$

Asi llegamos a que :

$$Sol(x^2 - dy^2 = \pm 1) \ = \ N^{-1}\{\pm 1\} = \mathcal{U}_{[\sqrt{d}]} = \{\pm 1\} \times \mathcal{U}^+_{[\sqrt{d}]}$$

Que dividiendo los casos nos queda:

$$Sol(x^2 - dy^2 = +1) \ = \ N^(-1)\{+1\} = \{\pm 1\} \times N^{-1}(+1)^+$$

$$Sol(x^2 - dy^2 = -1) \ = \ N^(-1)\{-1\} = \{\pm 1\} \times N^{-1}(-1)^+$$

Ademas:

$$N^{-1}(1) = \pm(N^{-1}(1)^{>1})^{\pm 1} \sqcup \{1\}$$
$$N^{-1}(-1) = \pm(N^{-1}(-1)^{>1})^{\pm 1}$$

Por lo tanto, el problema se reduce a calcular $N^{-1}(1)^{>1}$, $N^{-1}(1)^{>1}$. Asi se ha procedido, ya en el caso analizado. Análogamente en este se tiene: Si $x + \sqrt{d}y \in N^{-1}(-1)$, puesto que $x^2 - dy^2 = -1$:

$$0 < |x| < \sqrt{d}|y|$$

Por tanto tenemos la siguiente proposición:

Proposición 2.17.

$$N^{-1}(-1)^{+} = N^{-1}(-1) \cap \{x + \sqrt{d}y,\ y > 0\} \tag{2.3}$$

$$N^{-1}(-1)^{>1} = N^{-1}(-1) \cap \{x + \sqrt{d}y,\ x, y > 0\} \tag{2.4}$$

Demostración. Sea $x + \sqrt{d}y \in \mathbb{N}^{-1}(-1)$

$$x + \sqrt{d}y > 0 \leftrightarrow y > 0$$

ya que $|x| < \sqrt{d}|y|$.

$$x, y > 0 \ : \ x + \sqrt{d}y > 1$$

Si $x + \sqrt{d}y > 1$, por el apartado 2.3: $y > 0$. Si $x < 0$ entonces:

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

□

Ahora bien, para analizar el caso de $N^{-1}(-1)$ se debe, como en el caso $N^{-1}(1)$, analizar un grupo, y éste es $N^{-1}(\pm 1) = \mathcal{U}_{\mathbb{Z}[\sqrt{d}]}$ al que aplicando el corolario 2.10:

$$N^{-1}(\pm 1)^{+} \text{ cíclico infinito} \Rightarrow \exists \xi = min\ N^{-1}(\pm 1)^{>1}$$

Definición 2.18. Al mínimo ξ se le llama unidad fundamental de $\mathbb{Z}[\sqrt{d}]$, y cumple que $\langle \xi \rangle = N^{-1}(\pm 1)^{+}$

Como en el caso $N^{-1}(1)$, tal ξ mínimo existe:

$$\xi = x_0 + \sqrt{d}y_0,\ x_0, y_0 \text{ mínimos} > 0 \text{ en } N^{-1}(\pm 1)$$

ya que por la proposición anterior 2.17 junto con el corolario 2.10 dan:

$$N^{-1}(\pm 1)^{>1} = N^{-1}(\pm 1) \cap \{x + \sqrt{d}y,\ x, y > 0\}$$

Ahora bien:

$$(N^{-1}(\pm 1) : N^{-1}(1)) = (N^{-1}(\pm 1)^{+} : N^{-1}(1)^{+}) = 1 \text{ ó } 2 \tag{2.5}$$

según si la ecuación $x^2 - dy^2 = -1$ no tenga o tenga solución. En el primer caso(que no tenga solución): $\xi = \varepsilon$ solución fundamental de $x^2 - dy^2 = 1$. En cuanto al otro caso, en el que $x^2 - dy^2 = -1$ tiene solución, al ser el índice 2, $\xi \notin N^{-1}(1)^{+}$, por lo que:

$$\xi = minN^{-1}(-1)^{>1}$$

y se llama solución fundamental de $x^2 - dy^2 = -1$:

$$N^{-1}(-1)^+ = \{\xi^n,\ n \in \mathbb{Z} - 2\mathbb{Z}\}$$

Ademas $\xi^2 = \varepsilon$ solución fundamental de $x^2 - dy^2 = 1$.

El calculo efectivo de $N^{-1}(\pm 1)^+$ está relacionado con el algoritmo de las fracciones continuas de los irracionales cuadraticos(reales, en este caso). Pero los casos $N^{-1}(1)$, $N^{-1}(-1)$ deben ser analizados por separado.

Si $x + \sqrt{d}y \in N^{-1}(-1)^{>1}\ :\ x < \sqrt{d}y$ y análogamente se llega a que $\frac{x}{y}$ es un convergente a $\sqrt{d}$.

Por tanto

Proposición 2.19. *Si $x + \sqrt{d}y \in N^{-1}(\pm 1)^{>1}$, entonces $\frac{x}{y}$ es un convergente a $\sqrt{d}$*

Averigüemos qué convergentes a $\sqrt{d}$ son elementos de $N^{-1}(\pm 1)^{>1}$. El Teorema [[[[]]] puede ser ahora reformulado:

Teorema 2.20. *Siendo $\frac{p_n}{q_n}$ el n-esimo convergente entonces:*

$$p_n + \sqrt{d}q_n \in N^{-1}(\pm 1)^{>1} \leftrightarrow n = lm - 1 \begin{cases} n & impar\ para & +1 \\ n & par\ para & -1 \end{cases} \tag{2.6}$$

Por tanto:

a)

$$+1 : \begin{cases} m & par: & l = 1, 2, 3, \ldots \\ m & impar: & l = 2, 4, 6, \ldots \end{cases}$$

b)

$$-1 : \begin{cases} m & par: & no\ hay\ solución \\ m & impar: & l = 1, 3, 5, \ldots \end{cases}$$

Demostración. a) Hecho en el Teorema 2.16

b) Si $x + \sqrt{d}y \in N^{-1}(-1)_{>1}\ :\ \dfrac{x}{y} < \sqrt{d}$ y solo los convergentes pares son menores a $\sqrt{d}$. El resto del razonamiento es análogo a a) del Teorema 2.16 .

□

El caso $x^2 - dy^2 = k$, $k \in \dot{\mathbb{Z}}$ es más complicado. Así como $N^{-1}(-1) = \theta N^{-1}(1)$, con θ solución, no es cierto $N^{-1}(k) = \theta N^{-1}(1)$, con θ solución, ya que $N : \mathbb{Z}[\sqrt{d}] \to \dot{\mathbb{Z}}$ es solo un homomorfismo de monoides.

Analizaremos precisamente el siguiente caso de los cuerpos cuadráticos: $\mathcal{K} = \mathbb{Q}(\sqrt{d})$ $d \equiv 1(4)$

$$\mathcal{U}_{\mathcal{K}} = \frac{1}{2}N^{-1}(\pm 4)\ ,\ (N : \mathbb{Z}[\dot{\sqrt{d}}] \to \dot{\mathbb{Z}})$$
$$\frac{1}{2}Sol(x^2 - dy^2 = \pm 4)^+ = \frac{1}{2}N^{-1}(\pm 4)^+ = \langle n = \frac{1}{2}(a + \sqrt{d}b)\rangle$$
$$Sol(x^2 - dy^2 = \pm 1)^+ = N^{-1}(\pm 1)^+ = \langle \xi \rangle$$

n es la unidad fundamental de $\mathcal{K}$

ξ es la unidad fundamental de $\mathcal{K}[\sqrt{d}]$

Se verifica :

$$a, b \text{ pares} : \xi = n$$
$$a, b \text{ pares} : \xi = n^3$$

Por lo tanto la solución fundamental de $x^2 - dy^2 = \pm 4$ es $2n$. Además, puesto que $\frac{1}{2}N^{-1}(4) \subset \frac{1}{2}N^{-1})(\pm 2)$ (subgrupo de indice 2). La forma que la solución de $x^2 - dy^2 = 4$ es $2n$ ó $2n^2$ segun $x^2 - dy^2 = -4$ no tenga o tenga solución. Así

Proposición 2.21. *Con $d \equiv 1(4)$: $x^2 - dy^2 = \pm 4$ tiene infinitas soluciones.*

Esto se puede hallar si se calcula la unidad fundamental n de $\mathcal{K}$. Para ello no vale el procedimiento de fracciones continuas, pero se tiene otra .

Demostración. □

Veamos el caso general: Sea $\mathcal{H}$ subgrupo de un monoide $\mathcal{G}$. Entonces

$$x\mathcal{H},\ x \in \mathcal{G}$$

es una partición de $\mathcal{G}$. Sea $\mathcal{G} \to^f \mathcal{G}$ con f homomorfismo de monoides de núcleo $\mathcal{H}$, subgrupo de $\mathcal{G}$. Para $x' \in \mathcal{G}'$:

$$f^{-1}(x') = \bigcup_{f(x)=x'} x\mathcal{H}$$

El numero de clases pueden ser 0 ($f^{-1}(x') = \emptyset$), 1 (Cuando $\mathcal{G}$ es un grupo), e incluso ∞. La relación de equivalencia indicada por $\mathcal{G}$ por $\mathcal{H} = Ker(f)$ es más fina que la indicada por (f)

Para $N : \mathbb{Z}[\dot{\sqrt{d}}] \to \dot{\mathbb{Z}}$, $k \in \dot{\mathbb{Z}}$:

$$Sol(x^2 - dy^2 = k) = N^{-1}(k) = \bigcup_{N(\theta)=k} \theta N^{-1}(1)$$

Así las clases se llaman clases de soluciones de $x^2 - dy^2 = k$

Por lo tanto, para resolver $x^2 - dy^2 = k$, basta encontrar el representante de cada clase de soluciones:

Teorema 2.22. *Si $k > 0$, existe solo un numero finito de clases de soluciones de $x^2 - dy^2 = k$. Encontrar un representante de cada clase es un problema finito una vez que se ha calculado la solución fundamental, ε, de $x^2 - dy^2 = 1$.*

Demostración. □

El numero de clases de soluciones de $x^2 - dy^2 = k$ puede ser cero, es decir $x^2 - dy^2 = k$ no representa a k. Peroo esto es una cuestión de otra índole, enmarcada en el problema general de representación por formas binarias.

Si se quisiera entender este análisis de la forma $x^2 - dy^2$ a una forma binaria $f(x, y) = ax^2 + bxy + cy^2$. Ahora veamos ante todo que es semejante a una completa.

$$f(x, y) = aN(x + \alpha y),$$

Siendo α raíz de $ax^2 - bx + c = 0 : \alpha = \dfrac{b + \sqrt{\Delta}}{2a}$ Por lo tanto limitémonos al caso $a = 1$: $f(x, y) = x^2 + bxy + cy^2$.

$$Sol(f(x, y) = 1) = KerN \ : \ N : \mathbb{Z}\dot{[}\alpha] \to \dot{\mathbb{Q}}$$

Si ε es solución, lo es $\pm\varepsilon^{\pm 1}$, es decir, $\varepsilon = x + \alpha y$:

$$\pm(x + \alpha y) \ , \pm(x + by - \alpha y).$$

Pero ya que no se obtiene: (en el caso real: $\alpha \in \mathbb{R}$).

$$KerN^{>1} = KerN \cap \{x + \alpha y, \ x > 1, \ y > 0\},$$

Así:

$$x + \alpha y \in KerN^{>1} \ : \ x > \alpha y$$

relación de la cual, en el caso de la ecuación de Pell, se dedujo $\frac{x}{y}$ es convergente a α.

Vamos a analizarlo desde el punto de vista algebraico:

$$\mathcal{U}_{\mathbb{Q}(\alpha)} = N^{-1}\{\pm 1\} : \ N : R \dot{\to} \dot{\mathbb{Q}}$$

Siendo R anillo de enteros de $\mathbb{Q}(\alpha)$.

$$\alpha = \frac{b+\sqrt{\Delta}}{2} = \frac{b+k\sqrt{\Delta}}{\Delta_1},$$

(Con $\Delta = k^2\Delta_1$, Δ_1 libre de cuadrados):

$$\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{\Delta_1}) \ : \ R = \mathbb{Z}[\sqrt{\Delta_1}] \ si \ \Delta_1 \equiv 2 \text{ ó } 3 \ (4)$$

Ahora nos podemos plantear la pregunta de ¿Cuándo es $\mathbb{Z}[\sqrt{\Delta_1}] = \mathbb{Z}[\alpha]$?

Se deduce fácilmente, siempre y cuando $\Delta = 4\delta_1$.(Esto ocurre en la ecuación de Pell: $x^2 - dy^2$ con d libre de cuadrado : $\Delta = 4d$, $\Delta_1 = d$, $\alpha = \sqrt{d}$). En este caso:

$$Sol(f(x,y) = \pm 1) = \mathcal{U}_{\mathbb{Q}(\alpha)} = \mathcal{U}_{\mathbb{Q}(\sqrt{\Delta_1})} = Sol(x^2 - \Delta_1 y^2 = \pm 1)$$

Esto está calculado por fracciones continuas(el caso $= -1$ también [2]).(El teorema de las unidades dice que esto es un grupo cíclico. $Sol(= \pm 1)$ es subgrupo).

Todo esto sugiere "puentear"$\mathcal{U}_{\mathbb{Q}}(\alpha)$, de modo que aparte de evitar la restricción $\equiv 2$ ó 3 (4) y el caso $= -1$, se tiene un procedimiento más directo:

Puesto que el análisis de la Ecuación de Pell sólo precisa de que $d \notin \mathbb{Q}^2$, $d > 0$, la cuestión sigue siendo:

¿Cuándo $\mathbb{Z}[\alpha] = \mathbb{Z}[\sqrt{\Delta_1}]$, $\Delta = k^2\Delta_1$?: Siempre y cuando : $4|\Delta$, es decir $2|b$.

Por lo tanto sea $f(x,y) = x^2 + 2bxy + cy^2$, $b^2 > c$.

Así $\alpha = b + \sqrt{b^2 - c}$:

$$Sol(f(x,y) = 1) = KerN_{\mathbb{Z}[\alpha]} = KerN_{|}\mathbb{Z}[\dot{b^2} - c] = Sol(x^2 - (b^2 - c)y) = 1$$

De hecho $f(x,y)$ propiamente equivalente a $x^2 - (b^2 - c^2)y$.

Vamos a introducir todo esto en el contexto general de las formas cuadráticas binarias, en cuanto a l lenguaje, pero sin usar los resultados fuertes:

Para una base α, β de un cuerpo cuadrático K denotamos $F(\alpha,\beta) = N(\alpha x + \beta y)$, sin normalizar, y no como en la teoria general($F(\alpha,\beta) = [N(\alpha x + \beta y)/B(\alpha,\beta)]_S$). Si lo que pretendemos ahora es analizar la representación del 1 por $f(x,y) = ax^2 + bxy + cy^2$, tratando de generalizar el método empleado en la ecuación Pell, ante todo, como ya se ha visto:

$$f(x,y) = aF(1,\alpha), \ \alpha raiz \ de \ ax^2 - bx + c = 0, \ \alpha = \frac{b+\sqrt{D}}{2a}$$

imponemos la restricción $a = 1$. Pero, aún con esta restricción, ya se observó que no es viable extender el resultado de Pell para obtener $Sol(f(x,y) = 1) = KerN_{|\mathbb{Z}[\alpha]}$ mediante convergentes

de la representación en fracciones continuas de α: En efecto, hemos visto que para que $\mathbb{Z}[\alpha]$ sea el anillo de enteros de un cuerpo cuadrático real, estaríamos en el caso de Pell.

Por ello consideramos las ecuaciones de Pell: $x^2 - dy^2 = 1$, $0 < d \notin \mathbb{Q}^2$. Llamaremos a:

$$F(1, \sqrt{d}) = x^2 - dy^2,\ 0 < d \notin \mathbb{Q}^2,\ D = 4d$$

una *forma de Pell*. Combinando varias ecuaciones de Pell.

Tenemos que la ecuación de Pell está resuelta. Pero no la expresión por *formas de Pell*, salvo dentro del contexto general de representación por formas binarias. Aqui no estamos tratando esto sino salvo solamente la representación de 1, es decir la ecuación de Pell. A la clase (propia) de la *forma de Pell* la llamaremos *Clase de Pell*. Es una clase primitiva completa no definida. A su discriminante lo llamaremos *discriminante de Pell*: $0 < D \notin \mathbb{Q}^2$, $4|D$.

Considerando varias clases primitivas (dependiendo el numero de Clases de D) y exactamente una de Pell: los *discriminantes de Pell* son exactamente los discriminantes irreducibles($D \notin \mathbb{Q}^2$), no negativos ($0 < D$) y clasicamente enteros ($4|D$). Estas nociones de clases son invariantes en discriminantes.

De entre varias clases, primitivas o no ($D = 20$ es de *Pell* y $x^2 - 5y^2$, $2x^2 + 6xy + 2y^2$ están en él) que contienen al *discriminante de Pell* se trata de distinguir cual es la de *Pell*:

" En un *discriminante de Pell*, la *clase de Pell* es la única que contiene una forma con $a = 1$". Esto es consecuencia de la siguiente:

Proposición 2.23. *Sea $f(x, y) = x^2 + bxy + cy^2 = F(1, \alpha)$, α raiz de $x^2 - bx + c = 0$, una forma de discriminante D. Son equivalentes:*

i) $f(x, y)$ es propiamente equivalente a la forma de Pell.

ii) Existe $0 < d \notin \mathbb{Q}^2$, $\mathbb{Z}[\alpha] = \mathbb{Z}[\sqrt{d}]$

iii) D es discriminante de Pell.

(En el caso de $D = 4d$. Obviamente también que $\mathbb{Z}[\alpha] = (1, \alpha)$)

Demostración. Veamos las implicaciones

i)⇒iii) Obvio

ii)⇒i) Las bases $\{1, \alpha\}$, $\{1, \sqrt{d}\}$ del mismo módulo dan formas equivalentes: $F(1, \alpha) \sim F(1, \sqrt{d}) = x^2 - dy^2$. Puesto que el discriminante es D: $D = 4d$. Luego $\alpha = \dfrac{b + \sqrt{D}}{2} = \dfrac{b}{2} + \sqrt{d}$. Por lo tanto $\{1, \alpha\}$ y $\{1, \sqrt{d}\}$ son propiamente equivalentes.

iii)⇒ii) $\alpha = \dfrac{b+\sqrt{D}}{2} = \dfrac{b}{2} + \sqrt{d}$, haciendo $D = 4d$. Puesto que $\dfrac{b}{2} \in \mathbb{Z}$(Al ser $4|D$) se tiene que: $\mathbb{Z}[\alpha] = \mathbb{Z}[\sqrt{d}]$.

□

Dada una forma $f(x,y) = ax^2 + bxy + cy^2$ se calcula su discriminante. Si éste no es de Pell no hay nada que hacer por este camino. Si es de Pell y $a = 1$ está es la clase de Pell. En el caso de un a arbitrario, "$f(x,y)$ está en la clase de *Pell* si y solo si es propiamente equivalente a una forma con $a = 1$". Pero no disponemos de mejor procedimiento para averiguar si está en la clase de Pell.

Ejercicio 2.24. *Hallar la solución particular de la ecuación de Pell: $x^2 - dy^2 = 1$. Para $d = 7, 13, 41, 19, 14, 23$, usando el algoritmo de las fracciones continuas. Explica por qué este algoritmo es más eficiente que el cálculo directo.*

Bibliografía

[1] Aparicio, E.(1993) *Teoría de los números*, Univ País Vasco.

[2] Baker, A. (1984). *A concise introduction to the theory of numbers,* Cambridge Univ. Press.

[3] Cassels, J.W.S. and Fröhlich, A.(Eds), (1970), Algebraic number theory, Academic Press.

[4] Lang, S. (1970), *Algebraic number theory*, Addison Wesley.

[5] Leveque, W. J. (1977). *Fundamental of number theory*,Addison-Wesley.

[6] Neukirch, J.(1999), *Algebraic number theory*, Springer

[7] Sierpinski, W. (1988). *Elementary theory of numbers*, 2nd ed., North-Holland mathematical library ; 31, North-Holland, Amsterdam.

[8] Weiss, E. (1969). *Cohomology of groups*, Pure and applied mathematics (Academic Press) ; 34, Academic Press, New York.