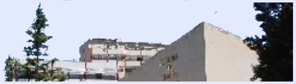
FRACCIONES CONTINUAS

¿Cómo aproximar un número eficientemente?

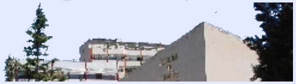
1. Introducción 5
2. Ejemplos de desarrollo 6
   Ejemplo 1 6
   Ejemplo 2 6
   Ejemplo 3 6
3. fcs puramente periódica 7
   Ejemplo 4 7
   Ejemplo 5 7
4. FCS periódicas 8
   Ejemplo 6 8
   Ejemplo 7 8
5. Otras FCS periódicas 9
   Ejemplo 8 9
   Ejemplo 9 9
   Ejemplo 10 10

ugr Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra



Ejemplo 11 10
Ejemplo 12 10
6. Fracciones continuas de racionales e irracionales 11
Teorema 1 12
Corolario 1 12
Teorema 2 13
Corolario 2 13
Corolario 3 13
7. Cálculo de convergentes. 14
Ejemplo 13 14
Ejemplo 14 14
Ejemplo 15 14
Ejemplo 16 15
8. Una aplicación. 15
9. Mas propiedades 16
Lema 1 16
10. Cálculo de FCS de irracionales cuadráticos 17
11. FCS de un irracional cuadrático 19
12. Aproximación de irracionales 20
Teorema 3 20
Teorema 4 22
Teorema 5 23
Corolario 4 24

Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

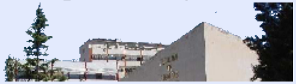


	Teorema 6	25
	Corolario 5	25
	Ejemplo 17	25
13.	Ecuaciones cuadráticas diofánticas	26
	Teorema 7	27
	Corolario 6	29
	Corolario 7	29
	Definición 1	29
	Ejemplo 18	29
14.	Caracterización de FCS periódicas	30
	Teorema 8	30
	Definición 2	31
	Ejemplo 19	31
	Teorema 9	31
	Corolario 8	32
	Corolario 9	33
	Teorema 10	34
	Teorema 11	35
	Corolario 10	35
	Teorema 12	36
	Teorema 13	36
	Corolario 11	36
	Ejemplo 20	36

Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

15. Aplicaciones 37
Ejemplo 21 38
Ejemplo 22 38
Ejemplo 23 39
Ejemplo 24 39
16. Ejercicios. 40
Ejercicio 1 40
17. Referencias. 40
40
18. Test de repaso. 40

Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra



Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

1. Introducción

Dado un número real $x \in \mathbb{R}$, su desarrollo en **fracción continua simple, FCS** es una sucesión de números enteros, $[q_0, q_1, q_2, \ldots]$, donde $q_0 = \lfloor x \rfloor$ es la parte entera de $x_0 = x$, que es negativa cuando x lo es, y el resto de los $q_i = \lfloor x_i \rfloor$ con $x_i = \frac{1}{x_{i-1} - q_{i-1}}$, definidos por inducción, son enteros positivos salvo que x sea racional. Equivale a las sucesivas igualdades

$$x = q_0 + \frac{1}{x_1},\ x_1 = q_1 + \frac{1}{x_2}, \ldots, x_i = q_i + \frac{1}{x_{i-1}}, \ldots$$

Se pueden resumir escribiendo una única igualdad con puntos suspensivos

$$x = q_0 + \cfrac{1}{q_1 + \frac{1}{q_2 + \cdots}}$$

Si x no es entero, $q_0 < x < q_0 + 1 \iff 0 < x - q_0 < 1 \iff 1 < \frac{1}{x - q_0} = x_1$. Claramente, para todo i, se tiene que la siguiente expresión es una FCS

$$x_i = q_i + \frac{1}{q_{i+1} + \cdots} = [q_i, q_{i+1}, q_{i+2}, \ldots]$$

Pero la que sigue es FC finita pero no simple porque x_r casi nunca es entero.

$$x = [q_0, q_1, \ldots, q_{r-1}, x_r] = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots + \frac{1}{x_r}}}}$$

Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

2. Ejemplos de desarrollo

Ejemplo 1. *Para* $x=\sqrt{2}$*, se tiene* $\sqrt{2}=1+(\sqrt{2}-1)=1+\frac{1}{1+\sqrt{2}}$*. Pero como*

$$1+\sqrt{2}=2+(\sqrt{2}-1)=2+\frac{1}{1+\sqrt{2}} \Rightarrow \sqrt{2}=1+\frac{1}{2+\frac{1}{1+\sqrt{2}}}$$

y se repite el último denominador, se tiene $\sqrt{2}=[1,2,2,\dots]$

Ejemplo 2. *Para* $x=\sqrt{3}$*, se tiene* $\sqrt{3}=1+(\sqrt{3}-1)=1+\frac{2}{1+\sqrt{3}}=1+\frac{1}{(1+\sqrt{3})/2}$ *entonces*

$$\frac{1+\sqrt{3}}{2}=\frac{2+(\sqrt{3}-1)}{2}=1+\frac{1}{1+\sqrt{3}} \Rightarrow \sqrt{3}=1+\frac{1}{1+\frac{1}{1+\sqrt{3}}}$$

$$1+\sqrt{3}=2+(\sqrt{3}-1)=2+\frac{1}{(1+\sqrt{3})/2} \Rightarrow \sqrt{3}=1+\frac{1}{1+\frac{1}{2+\frac{1}{(1+\sqrt{3})/2}}}$$

y este denominador, $(1+\sqrt{3})/2$*, se repite con el primero, entonces* $\sqrt{3}=[1,\overline{1,2},\overline{1,2},\dots]$

Ejemplo 3. *Para* $x=\sqrt{5}$*, se tiene* $\sqrt{5}=2+(\sqrt{5}-2)=2+\frac{1}{\sqrt{5}+2}$ *entonces*

$$\sqrt{5}+2=4+(\sqrt{5}-2)=4+\frac{1}{\sqrt{5}+2} \Rightarrow \sqrt{5}=2+\frac{1}{4+\frac{1}{\sqrt{5}+2}}$$

y como este denominador, $\sqrt{5}+2$ *se repite, se tiene* $\sqrt{5}=[2,4,4,\dots]$

3. FCS PURAMENTE PERIÓDICA

Ejemplo 4. *Para* $x = \frac{a+\sqrt{a^2+4}}{2}$*, se tiene*

$$\frac{a+\sqrt{a^2+4}}{2} = \frac{2a+\sqrt{a^2+4}-a}{2} = a + \frac{\sqrt{a^2+4}-a}{2} = a + \frac{4}{2(\sqrt{a^2+4}+a)} = a + \frac{1}{\frac{\sqrt{a^2+4}+a}{2}} =$$

$$= a + \frac{1}{x}$$

y como se repite, $x = (a+\sqrt{a^2+4})/2$*, se tiene*

$$x = a + \cfrac{1}{a + \cfrac{1}{a + \cfrac{1}{\ddots}}} = [a, a, a, \ldots]$$

Recíprocamente, si $x = [a, a, a, \ldots]$ *con* a *entero positivo, entonces*

$$x = a + \frac{1}{x} = \frac{ax+1}{x} \Leftrightarrow x^2 - ax - 1 = 0 \Rightarrow x = \frac{a \pm \sqrt{a^2+4}}{2}$$

pero como $0 < a < x$*, se tiene necesariamente que* $x = \frac{a+\sqrt{a^2+4}}{2}$

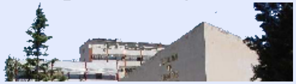
Ejemplo 5. $[1,1,1,\ldots] = \frac{1+\sqrt{5}}{2} \simeq 1.618$ *Número Aúreo*

$$[2,2,2,\ldots] = \frac{2+\sqrt{8}}{2} = 1+\sqrt{2}$$

$$[3,3,3,\ldots] = \frac{3+\sqrt{13}}{2}$$

Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra



4. FCS periódicas

Para $\sqrt{a^2+1}$, se tiene

$$\sqrt{a^2+1} = a + (\sqrt{a^2+1} - a) = a + \frac{1}{\sqrt{a^2+1}+a}$$

$$\sqrt{a^2+1} + a = 2a + (\sqrt{a^2+1} - a) = 2a + \frac{1}{\sqrt{a^2+1}+a}$$

$$\sqrt{a^2+1} + a = 2a + (\sqrt{a^2+1} - a) = 2a + \frac{1}{\sqrt{a^2+1}+a}$$

y como se repite, $\sqrt{a^2+1}+a$, se tiene $\sqrt{a^2+1} = [a, 2a, 2a, \dots]$

Ejemplo 6. $\sqrt{5} = [2, 4, 4, \dots]$, $\quad \sqrt{10} = [3, 6, 6, \dots]$, $\quad \sqrt{17} = [4, 8, 8, \dots]$, *etc.*

Para $\sqrt{a^2+2}$, *se tiene*

$$\sqrt{a^2+2} = a + (\sqrt{a^2+2} - a) = a + \frac{2}{\sqrt{a^2+2}+a}$$

$$\frac{\sqrt{a^2+2}+a}{2} = \frac{2a+\sqrt{a^2+2}-a}{2} = a + \frac{1}{\sqrt{a^2+2}+a}$$

$$\sqrt{a^2+2} + a = 2a + (\sqrt{a^2+2} - a) = 2a + \frac{2}{\sqrt{a^2+2}+a}$$

y como se repite, $(\sqrt{a^2+2}+a)/2$, *se tiene* $\sqrt{a^2+2} = [a, a, 2a, a, 2a, \dots]$

Ejemplo 7. $\sqrt{6} = [2, \overline{2, 4}, \dots]$, $\quad \sqrt{11} = [3, \overline{3, 6}, \dots]$, $\quad \sqrt{18} = [4, \overline{4, 8}, \dots]$, *etc.*

ugr Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

5. Otras FCs periódicas

Para $\sqrt{a^2-1}$, se tiene

$$\sqrt{a^2-1} = a-1+(\sqrt{a^2-1}-(a-1)) = a-1+\frac{2a-2}{\sqrt{a^2-1}+a-1} = a-1+\frac{1}{\frac{\sqrt{a^2-1}+a-1}{2(a-1)}}$$

$$\frac{\sqrt{a^2-1}+a-1}{2(a-1)} = \frac{2(a-1)+(\sqrt{a^2-1}-(a-1))}{2(a-1)} = 1+\frac{1}{\sqrt{a^2-1}+a-1}$$

$$\sqrt{a^2-1}+a-1 = 2(a-1)+(\sqrt{a^2-1}-(a-1)) = 2(a-1)+\frac{2a-2}{\sqrt{a^2-1}+a-1}$$

y como se repite, $\frac{2a-2}{\sqrt{a^2-1}+a-1}$, se tiene $\sqrt{a^2-1} = [a-1, \overline{1, 2(a-1)}, \dots]$

Ejemplo 8. *Dándole valores al parámetro a se obtienen*

$$\sqrt{3} = [1, \overline{1,2}, \dots], \sqrt{8} = [2, \overline{1,4}, \dots], \sqrt{15} = [3, \overline{1,6}, \dots], \sqrt{24} = [4, \overline{1,8}, \dots], \ \textit{etc.}$$

Ejemplo 9. *Análogamente se demuestra*

$\sqrt{a^2-2} = [a-1, \overline{1, a-2, 1, 2(a-1)}, \dots]$. *Y dando valores al parámetro*
$\sqrt{7} = [2, \overline{1,1,1,4}, \dots], \sqrt{14} = [3, \overline{1,2,1,6}, \dots], \sqrt{23} = [4, \overline{1,3,1,8}, \dots]$, *etc.*

Como se observa, cuanto mas se acerca un número a una raíz cuadrada más simple es su FC. Sin embargo, se pueden obtener ejemplos de desarrollos de cualquier longitud. Para $d \le 1000$, el periodo más largo es de longitud 60.

$$\sqrt{919} = [30, 3, 5, 1, 2, 1, 2, 1, 1, 1, 2, 3, 1, 19, 2, 3, 1, 1, 4, 9, 1, 7, 1, 3, 6, 2, 11, 1, 1, 1,$$

$29, 1, 1, 1, 11, 2, 6, 3, 1, 7, 1, 9, 4, 1, 1, 3, 2, 19, 1, 3, 2, 1, 1, 1, 2, 1, 2, 1, 5, 3, 60]$

Ejemplo 10. *Como* $x = [1, 1, 1, \ldots] = \frac{1+\sqrt{5}}{2}$, *la FCS* $y = [2, 1, 1, \ldots]$ *también se puede evaluar*

$$y = 2 + \frac{1}{x} = 2 + \frac{2}{1+\sqrt{5}} = 2\left(1 + \frac{1-\sqrt{5}}{-4}\right) = 2\left(\frac{3+\sqrt{5}}{4}\right) = \frac{3+\sqrt{5}}{2}$$

Ejemplo 11. *La FCS* $x = [2, 1, 2, 1, \ldots]$ *se puede evaluar por ser periódica ya que*

$$x = 2 + \frac{1}{1+\frac{1}{x}} = 2 + \frac{x}{x+1} = \frac{3x+2}{x+1} \Leftrightarrow x^2 - 2x - 2 = 0 \Rightarrow x = 1 \pm \sqrt{3}$$

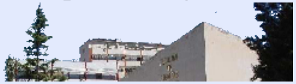
y como claramente $2 < x$, *la FCS* x *es positiva y entonces* $x = 1 + \sqrt{3}$.

Ejemplo 12. *La FCS* $x = [1, 3, 1, 2, 1, 2, \ldots]$ *se puede evaluar ya que se tiene* $x = 1 + \frac{1}{3+\frac{1}{y}} = 1 + \frac{y}{3y+1} = \frac{4y+1}{3y+1}$ *con* $y = [1, 2, 1, 2, \ldots]$ *y como* $1 < y$

$$y = 1 + \frac{1}{2+\frac{1}{y}} = 1 + \frac{y}{2y+1} = \frac{3y+1}{2y+1} \Leftrightarrow 2y^2 - 2y - 1 = 0 \Rightarrow y = \frac{1+\sqrt{3}}{2}$$

$$\textit{Finalmente, } x = \frac{4y+1}{3y+1} = \frac{4\frac{1+\sqrt{3}}{2}+1}{3\frac{1+\sqrt{3}}{2}+1} = 3 - \sqrt{3}$$

Enrique R. Aznar
Dpto. de Álgebra



Página web personal
Página de Abertura
Contenido
◀◀ ▶▶
◀ ▶

Atrás
Pantalla grande/pequeña
Cerrar

6. Fracciones continuas de racionales e irracionales

Una fracción continua simple, $x = [q_0, q_1, q_2, \dots, q_r] = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots + \cfrac{1}{q_r}}}}$, es finita si y sólo si $x = \frac{a}{b}$, $a, b \in \mathbb{Z}$, es un número racional. Se pueden tomar, b positivo y a, b primos entre si. En ese caso, los q_i son **cocientes parciales** que se obtienen al aplicar el AE para el cálculo del $\operatorname{mcd}(a, b) = 1$.

Como $[q_{r-1}, q_r] = q_{r-1} + \frac{1}{q_r}$ y $q_r = q_r - 1 + 1$, se tiene que

$$\left[q_0, q_1, q_2, \dots, q_{r-1} + \frac{1}{q_r}\right] = [q_0, q_1, q_2, \dots, q_r] = [q_0, q_1, q_2, \dots, q_r - 1, 1]$$

Pero la representación es única si exigimos que los q_i sean enteros y $1 < q_i$.

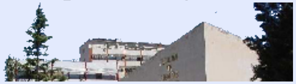
Equivalentemente, una FCS es infinita si y sólo si representa un número irracional x. En este caso, tienen sentido los números racionales sucesivos de su descomposición que llamamos sus **convergentes**:

$$r_i = \frac{A_i}{B_i} = [q_0, q_1, q_2, \dots, q_i]$$

Como por definición, $\begin{cases} [q_0] = q_0 \Longrightarrow r_0 = \frac{A_0}{B_0} = \frac{q_0}{1} \Longrightarrow A_0 = q_0,\ B_0 = 1 \\ [q_0, q_1] = q_0 + \frac{1}{q_1} = \frac{q_1 q_0 + 1}{q_1} \Longrightarrow A_1 = q_1 q_0 + 1,\ B_1 = q_1 \end{cases}$

Si definimos, $A_{-1} = 1$, $B_{-1} = 0$. Entonces, $\begin{cases} A_1 = q_1 q_0 + 1 = q_1 A_0 + A_{-1} \\ B_1 = q_1 = q_1 B_0 + B_{-1} \end{cases}$

Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra



Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

Son el primer caso de las ecuaciones recursivas siguientes

$$\begin{array}{ll} A_i = q_i A_{i-1} + A_{i-2}, & A_{-1} = 1, A_0 = q_0 \\ B_i = q_i B_{i-1} + B_{i-2}, & B_{-1} = 0, B_0 = 1 \end{array}$$

que permiten demostrar para cualquier $x \in \mathbb{R}$ y cualquier natural $n \geq 1$

Teorema 1. $[q_0, q_1, q_2, \ldots, q_{n-1}, x] = \frac{xA_{n-1}+A_{n-2}}{xB_{n-1}+B_{n-2}}$

Demostración: Para $n = 1$, se tiene $[q_0, x] = q_0 + \frac{1}{x} = \frac{xq_0+1}{x} = \frac{xA_0+A_{-1}}{xB_0+B_{-1}}$
Ahora por inducción, lo suponemos para $n-1$ y entonces

$$[q_0, q_1, q_2, \ldots, q_n, x] = [q_0, q_1, q_2, \ldots, q_{n-1}, q_n + \tfrac{1}{x}] = \frac{(q_n+\frac{1}{x})A_{n-1}+A_{n-2}}{(q_n+\frac{1}{x})B_{n-1}+B_{n-2}} =$$
$$= \frac{x(q_nA_{n-1}+A_{n-2})+A_{n-1}}{x(q_nB_{n-1}+B_{n-2})+B_{n-1}} = \frac{xA_n+A_{n-1}}{xB_n+B_{n-1}}$$

Por tanto, si tomamos $x = q_n \in \mathbb{Z}$, tenemos $r_n = \frac{A_n}{B_n} = [q_0, q_1, q_2, \ldots, q_n]$ y

Corolario 1. *Los convergentes de un número real pueden calcularse por las ecuaciones en recurrencia anteriores.*

Demostraremos que los convergentes de un $\alpha \in \mathbb{R}$ tienen por límite α y forman dos sucesiones encajadas con α en medio:

$$r_0 < r_2 < r_4 < \cdots < \alpha < \cdots < r_5 < r_3 < r_1$$

Lo que se llama una **cortadura de Dedekind** para un irracional α. En efecto

Teorema 2. *Los numeradores y denominadores, de los convergentes de una FCS, para todo i satisfacen*

$$A_{i-1}B_i - A_iB_{i-1} = (-1)^i \iff \frac{A_{i-1}}{B_{i-1}} - \frac{A_i}{B_i} = \frac{(-1)^i}{B_iB_{i-1}} \iff r_i - r_{i-1} = \frac{(-1)^{i-1}}{B_iB_{i-1}}$$

Demostración: Por inducción, el primer caso es inmediato

$$A_{-1}B_0 - A_0B_{-1} = 1 - 0 = 1 = (-1)^0$$

y si suponemos $A_{i-1}B_i - A_iB_{i-1} = (-1)^i$, entonces

$$A_iB_{i+1} - A_{i+1}B_i = A_i(q_{i+1}B_i + B_{i-1}) - (q_{i+1}A_i + A_{i-1})B_i =$$
$$= A_iB_{i-1} - A_{i-1}B_i = -(-1)^i = (-1)^{i+1}$$

Corolario 2. $(A_n, B_n) = 1$ *son primos entre si y la fracción* $\frac{A_n}{B_n}$ *está reducida.*

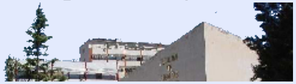
Corolario 3. $A_iB_{i-2} - A_{i-2}B_i = (-1)^i q_i \iff r_i - r_{i-2} = \frac{(-1)^i q_i}{B_iB_{i-2}}$

Demostración:La equivalencia es consecuencia de que $B_iB_{i-2} \neq 0$ y

$$A_iB_{i-2} - A_{i-2}B_i = (q_iA_{i-1} + A_{i-2})B_{i-2} - A_{i-2}(q_iB_{i-1} + B_{i-2}) =$$
$$= q_i(A_{i-1}B_{i-2} - A_{i-2}B_{i-1}) = q_i(-1)^{i-2} = q_i(-1)^i$$

Una FCS finita es un racional x/y, su última convergente es x/y y su penúltima convergente a/b satisface $bx - ay = (-1)^n$ donde n es el número de convergentes. Por tanto, el cálculo de convergentes proporciona un método para calcular soluciones a algunas ecuaciones diofánticas enteras.

ugr Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra



7. Cálculo de convergentes.

Observamos que los A_i B_i tienden a infinito rápidamente ya que satisfacen la misma ecuación en recurrencia con distintos parámetros iniciales.

$$\begin{array}{ll} A_i = q_i A_{i-1} + A_{i-2}, & A_{-1} = 1, A_0 = q_0 \\ B_i = q_i B_{i-1} + B_{i-2}, & B_{-1} = 0, B_0 = 1 \end{array}$$

Las fórmulas recursivas anteriores dan lugar a cálculos repetitivos que se pueden tabular

$$\begin{array}{cccccccc} & q_1 & q_2 & \dots & q_{s-1} & q_s & q_{s+1} & \dots \\ \frac{1}{0} & \frac{q_0}{1} & \frac{q_1 q_0 + 1}{q_1 \cdot 1 + 0} & \dots & \frac{A_{s-2}}{B_{s-2}} & \frac{A_{s-1}}{B_{s-1}} & \frac{q_s A_{s-1} + A_{s-2}}{q_s B_{s-1} + B_{s-2}} & \dots \end{array}$$

Ejemplo 13. *Para el número aúreo* $\varphi = [1, 1, 1, \dots] = \frac{1+\sqrt{5}}{2}$ *los primeros 7 convergentes son*

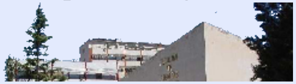
$$\begin{array}{cccccccc} & 1 & 1 & 1 & 1 & 1 & 1 & \dots \\ \frac{1}{0} & \frac{1}{1} & \frac{2}{1} & \frac{3}{2} & \frac{5}{3} & \frac{8}{5} & \frac{13}{8} & \dots \end{array}$$

Ejemplo 14. *Para el número* $[2, 2, 2, \dots] = 1 + \sqrt{2}$ *sus primeros convergentes son*

$$\begin{array}{cccccccc} & 2 & 2 & 2 & 2 & 2 & 2 & \dots \\ \frac{1}{0} & \frac{2}{1} & \frac{5}{2} & \frac{12}{5} & \frac{29}{12} & \frac{70}{29} & \frac{169}{70} & \dots \end{array}$$

ugr Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra



Ejemplo 15. *Para el número* $[3,3,3,\dots] = \frac{3+\sqrt{13}}{2}$ *sus primeros convergentes son*

$$\begin{array}{cccccccc} & 3 & 3 & 3 & 3 & 3 & 3 & \dots \\ \frac{1}{0} & \frac{3}{1} & \frac{10}{3} & \frac{33}{10} & \frac{109}{33} & \frac{360}{109} & \frac{1189}{360} & \dots \end{array}$$

Ejemplo 16. *Para el número* $\sqrt{3} = [1,\overline{1,2},\overline{1,2},\dots]$ *sus primeros convergentes son*

$$\begin{array}{ccccccccc} & 1 & 2 & 1 & 2 & 1 & 2 & 1 & \dots \\ \frac{1}{0} & \frac{1}{1} & \frac{2}{1} & \frac{5}{3} & \frac{7}{4} & \frac{19}{11} & \frac{26}{15} & \frac{71}{41} & \dots \end{array}$$

8. Una aplicación.

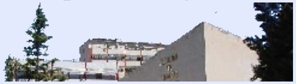
Calcular el inverso de 8 módulo 13 equivale a resolver $8x - 13y = 1$.
Como los convergentes del racional $13/8$ son

$$\begin{array}{cccccccc} & 3 & 3 & 3 & 3 & 3 & 3 & \dots \\ \frac{1}{0} & \frac{1}{1} & \frac{2}{1} & \frac{3}{2} & \frac{5}{3} & \frac{8}{5} & \frac{13}{8} & \dots \end{array}$$

el penúltimo convergente da $8*8-13*5 = (-1)^{6+1} = -1$.
Tomando módulo 13, se tiene

$$8^{-1} \equiv -8 \equiv 5 \pmod{13}$$

Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra



9. Mas propiedades

Dada una FC finita $[q_0, q_1, q_2, \dots, q_{r-1}, q_r]$ y un número real cualquiera x. Como

$$[q_0, x] = q_0 + \frac{1}{x} = \frac{xq_0 + 1}{x} = \frac{xA_0 + A_{-1}}{xB_0 + B_{-1}}$$

Si suponemos por inducción

$$[q_0, q_1, q_2, \dots, q_{r-1}, x] = \frac{xA_{r-1} + A_{r-2}}{xB_{r-1} + B_{r-2}}$$

entonces

$$[q_0, q_1, q_2, \dots, q_r, x] = [q_0, q_1, q_2, \dots, q_r + \frac{1}{x}] = \frac{(q_r + 1/x)A_{r-1} + A_{r-2}}{(q_r + 1/x)B_{r-1} + B_{r-2}} =$$

$$\frac{x(q_r A_{r-1} + A_{r-2}) + A_{r-1}}{x(q_r B_{r-1} + B_{r-2}) + B_{r-1}} = \frac{xA_r + A_{r-1}}{xB_r + B_{r-1}}$$

Por tanto,

Lema 1. *La igualdad* $[q_0, q_1, q_2, \dots, q_r, x] = \frac{xA_r + A_{r-1}}{xB_r + B_{r-1}}$ *es cierta para todo* $r \in \mathbb{N}$ *y todo* $x \in \mathbb{R}$*. En particular si* $x = q_{r+1}$ *es entero positivo, se tiene que una FCS finita coincide con su último convergente*

$$[q_0, q_1, q_2, \dots, q_r, q_{r+1}] = \frac{q_{r+1}A_r + A_{r-1}}{q_{r+1}B_r + B_{r-1}} = \frac{A_{r+1}}{B_{r+1}}$$

Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

10. Cálculo de FCS de irracionales cuadráticos

Si $\alpha \in \mathbb{R}$ es irracional y $q_0 = \lfloor \alpha \rfloor$, $\alpha_0 = \alpha$, por inducción se obtiene la FCS

$$q_i = \lfloor \alpha_i \rfloor, \qquad \alpha_i = \frac{1}{\alpha_{i-1} - q_{i-1}}$$

Si $\alpha = \frac{b+\sqrt{d}}{c}$, es irracional el método puede hacerse más eficiente. En particular, a, b, c son enteros con, $0 < b$, no cuadrado perfecto. Multiplicando numerador y denominador por cualquier múltiplo entero de $|c|$, podemos hacer que $c|(d-b^2)$. Decimos que α está en **forma normal** cuando

$$\alpha_0 = \alpha = \frac{P_0 + \sqrt{d}}{Q_0}, \text{ tal que } Q_0|(d-P_0^2) \Rightarrow Q_{-1} = \frac{d-P_0^2}{Q_0} \Leftrightarrow Q_{-1}Q_0 = d - P_0^2$$

Ahora, por inducción suponemos $\alpha_i = \frac{P_i+\sqrt{d}}{Q_i}$ tal que $Q_{i-1}Q_i = d - P_i^2$, y definimos $q_i = \lfloor \alpha_i \rfloor$, también definimos $P_{i+1} = q_i Q_i - P_i$ y

$$Q_i Q_{i+1} = d - P_{i+1}^2 \Longleftrightarrow Q_{i+1} = \frac{d-P_{i+1}^2}{Q_i} = \frac{d-P_i^2}{Q_i} + 2q_iP_i - q_i^2 Q_i =$$
$$= Q_{i-1} - q_i(q_iQ_i - P_i) + q_iP_i = Q_{i-1} - q_iP_{i+1} + q_iP_i = Q_{i-1} + q_i(P_i - P_{i+1})$$

O sea, $Q_iQ_{i+1} = d - P_{i+1}^2 \Longleftrightarrow Q_{i+1} = Q_{i-1} + q_i(P_i - P_{i+1})$.

Ahora, definimos $\alpha_{i+1} = \frac{P_{i+1}+\sqrt{d}}{Q_{i+1}}$ y tenemos

$$\alpha_i = \frac{P_i + \sqrt{d}}{Q_i} = q_i + \frac{\sqrt{d} - (q_iQ_i - P_i)}{Q_i} = q_i + \frac{\sqrt{d} - P_{i+1}}{Q_i} = q_i + \frac{d - P_{i+1}^2}{Q_i(P_{i+1} + \sqrt{d})} =$$

$$= q_i + \frac{Q_{i+1}}{(P_{i+1}+\sqrt{d})} = q_i + \frac{1}{\frac{P_{i+1}+\sqrt{d}}{Q_{i+1}}} = q_i + \frac{1}{\frac{P_{i+1}+\sqrt{d}}{Q_{i+1}}} \Rightarrow \alpha_i = q_i + \frac{1}{\alpha_{i+1}}$$

O sea, hemos demostrado que la FCS de $\alpha_0 = \alpha = \frac{P_0+\sqrt{d}}{Q_0}$ es

$$\alpha = [q_0, q_1, q_2, \dots, q_{i+1}, \dots]$$

Además, el cálculo de las partes enteras, q_{i+1}, puede hacerse sin aritmética de punto flotante con la fórmula

$$q_{i+1} = \lfloor \alpha_{i+1} \rfloor = \left\lfloor \frac{P_{i+1}+\sqrt{d}}{Q_{i+1}} \right\rfloor = \left\lfloor \frac{P_{i+1}+\left\lfloor\sqrt{d}\right\rfloor}{Q_{i+1}} \right\rfloor = Quot(P_{i+1}+\left\lfloor\sqrt{d}\right\rfloor, Q_{i+1}) = m$$

ya que se tienen las desigualdades siguientes

$$P_{i+1} + \left\lfloor\sqrt{d}\right\rfloor = mQ_{i+1} + r, \quad 0 \le r < Q_{i+1} \Rightarrow r+1 \le Q_{i+1} \Rightarrow$$

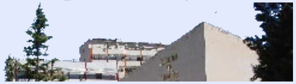
$$P_{i+1}+\sqrt{d} = P_{i+1}+\left\lfloor\sqrt{d}\right\rfloor+\delta = mQ_{i+1}+r+\delta < mQ_{i+1}+r+1 \le mQ_{i+1}+Q_{i+1} \Rightarrow$$

$$mQ_{i+1} < P_{i+1} + \left\lfloor\sqrt{d}\right\rfloor < P_{i+1} + \sqrt{d} < mQ_{i+1} + Q_{i+1}$$

Para el cálculo de $\left\lfloor\sqrt{d}\right\rfloor$ se puede usar un algoritmo sencillo que usa aritmética entera y la única división completa se hace al principio en el cálculo de $Q_{-1} = \frac{d-P_1^2}{Q_0}$ (aquí no se aplica la última fórmula recursiva).

Universidad de Granada

Enrique R. Aznar
Dpto. de Álgebra



ugr Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

11. FCS DE UN IRRACIONAL CUADRÁTICO

Así, si $\alpha = \frac{P+\sqrt{d}}{Q}$ con $Q|(d-P^2)$, entonces, en el paso i-ésimo de la FCS de α se tiene $q_i = \lfloor \alpha_i \rfloor$

$$\alpha_i = \frac{P_i + \sqrt{d}}{Q_i} = q_i + \frac{\sqrt{d} - (q_i Q_i - P_i)}{Q_i} = q_i + \frac{\sqrt{d} - P_{i+1}}{Q_i}$$

y por la definición de q_i, $0 < \frac{\sqrt{d}-P_{i+1}}{Q_i} < 1 \Rightarrow P_{i+1} < \sqrt{d}$

Además, de la definición recursiva

$$P_{i+1} = q_i Q_i - P_i \Leftrightarrow Q_i = \frac{P_i + P_{i+1}}{q_i} < 2\sqrt{d}$$

Por tanto, el número total de fracciones $\frac{P_i+\sqrt{D}}{Q_i}$ que aparecen en el desarrollo en FCS de un irracional cuadrático está acotado por el producto de ambas

$$\lfloor\sqrt{d}\rfloor 2 \lfloor\sqrt{d}\rfloor < 2d$$

Esto significa que como máximo en $2d$ pasos encontraremos una fracción α_i que ya ha aparecido antes y por tanto **la FCS de un irracional cuadrático es periódica con periodo como máximo** $2d-1$.

La longitud del periodo máximo nunca alcanza $2d-1$, ya que para $d > 7$ se puede demostrar que es menor que $0.72 \log_2(d)\sqrt{d}$

Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

12. Aproximación de irracionales

Dado un irracional $\alpha \in \mathbb{R}$, sabemos que sus convergentes $r_i = \frac{A_i}{B_i}$ son racionales que aproximan α. De hecho, r_i es la mejor de todas las aproximaciones racionales con denominador menor o igual que B_i como demuestra el sig.

Teorema 3. *Si $\frac{a}{b} \in \mathbb{Q}$, con $0 < b$ y $\frac{A_i}{B_i}$ los convergentes de un irracional $\alpha \in \mathbb{R}$. Entonces, para todo $n \geq 1$ se tiene*

i) $|b\alpha - a| < |B_n\alpha - A_n| \Longrightarrow B_{n+1} \leq b$
ii) $\left|\alpha - \frac{a}{b}\right| < \left|\alpha - \frac{A_n}{B_n}\right| \Longrightarrow B_n < b$

Demostración: Primero demostramos que i) implica ii). En caso contrario, existirá un $\frac{a}{b} \in \mathbb{Q}$, con $0 < b \leq B_n$ tal que multiplicando las desigualdades

$$\left.\begin{array}{rcl} \left|\alpha - \frac{a}{b}\right| & < & \left|\alpha - \frac{A_n}{B_n}\right| \\ b & \leq & B_n \end{array}\right\} \Longrightarrow |b\alpha - a| < |B_n\alpha - A_n| \Longrightarrow B_{n+1} \leq b$$

Absurdo, porque $b \leq B_n < B_{n+1} \leq b$. Luego i) implica ii).

Demostraremos i) por reducción al absurdo. Suponemos lo contrario. O sea

$$|b\alpha - a| < |B_n\alpha - A_n|, \quad B_{n+1} > b$$

y consideramos el s.l. que tiene determinante $A_nB_{n+1} - A_{n+1}B_n = (-1)^n \neq 0$

$$\left.\begin{array}{l} xA_n + yA_{n+1} = a \\ xB_n + yB_{n+1} = b \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} x = (-1)^n(aB_{n+1} - bA_{n+1}) \in \mathbb{Z} \\ y = (-1)^n(bA_n - aB_n) \in \mathbb{Z} \end{array}\right\}$$

Además, $x, y \neq 0$ ya que en caso contrario

$$\text{Si } x = 0 \Longrightarrow b = yB_{n+1} \Longrightarrow 0 < y \Longrightarrow b < B_{n+1} \text{ Absurdo}$$

$$\begin{array}{l} \text{Si } y = 0 \Longrightarrow a = xA_n,\ b = xB_n \Longrightarrow \\ |b\alpha - a| = |xB_n\alpha - xA_n| = |x||B_n\alpha - A_n| \geq |B_n\alpha - A_n| \text{ Absurdo} \end{array}$$

También x, y tienen signos opuestos ya que

$$\begin{array}{l} \text{Si } y < 0 \Longrightarrow xB_n = b - yB_{n+1} > 0 \Longrightarrow x > 0 \\ \text{Si } y > 0 \text{ como } B_{n+1} > b \Longrightarrow yB_{n+1} > b \Longrightarrow xB_n < 0 \Longrightarrow x < 0 \end{array}$$

Ahora, como convergentes sucesivas están una por debajo y otra por arriba de α las diferencias $B_n\alpha - A_n$ y $B_{n+1}\alpha - A_{n+1}$ tienen signos opuestos. Por tanto, $x(B_n\alpha - A_n)$ y $y(B_{n+1}\alpha - A_{n+1})$ tienen el mismo signo.

Finalmente, sustituyendo las ecuaciones del s.l. que definen a x, y

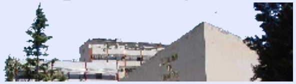
$$\alpha b - a = \alpha(xB_n + yB_{n+1}) - xA_n + yA_{n+1} = x(B_n\alpha - A_n) + y(B_{n+1}\alpha - A_{n+1})$$

Y tomando valor absoluto se obtiene una contradicción que demuestra todo:

$$|\alpha b - a| = |x(B_n\alpha - A_n)| + |y(B_{n+1}\alpha - A_{n+1})| > |x||B_n\alpha - A_n| \geq |B_n\alpha - A_n|$$

Después de este teorema técnico podemos dar una condición para que un racional a/b sea una convergente de un irracional $\alpha \in \mathbb{R}$.

ugr Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra



Primero vemos una desigualdad que satisfacen casi todos los convergentes de un irracional $\alpha \in \mathbb{R}$. Como los denominadores son enteros positivos que crecen estrictamente excepto posiblemente los 2 primeros. Entonces, para todo $n \geq 2$ se tiene que $2 \leq B_{n+1}$ y por tanto

$$\left|\alpha - \frac{A_n}{B_n}\right| < \frac{1}{B_n B_{n+1}} < \frac{1}{2B_n}$$

El recíproco es el importante

Teorema 4. ***Caracterización de convergentes***: *Si $\alpha \in \mathbb{R}$ irracional, $\frac{A_i}{B_i}$ son sus convergentes y $\frac{a}{b} \in \mathbb{Q}$, con $0 < b$. Entonces, se tiene*

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{2b^2} \Longrightarrow \frac{a}{b} = \frac{A_n}{B_n} \text{ para algún } n \in \mathbb{N}$$

Demostración: Si $\frac{a'}{b'} = \frac{ca}{cb} = \frac{a}{b}$ con $(a, b) = 1$ y $1 \leq c$. Entonces,

$$\left|\alpha - \frac{a}{b}\right| = \left|\alpha - \frac{a'}{b'}\right| < \frac{1}{2b'^2} < \frac{1}{2b^2}$$

y basta demostrar el teorema para $\frac{a}{b}$ con a y b primos entre si.

Como la sucesión B_n es estrictamente creciente a partir de $n = 2$ y empieza en 1, existe el mínimo natural n tal que $B_n \leq b < B_{n+1}$. Por el teorema anterior si $|b\alpha - a| < |B_n\alpha - A_n|$ entonces $B_{n+1} \leq b$. Luego para este n,

$$|B_n\alpha - A_n| \leq |b\alpha - a| < \frac{1}{2b} \Longrightarrow \left|\alpha - \frac{A_n}{B_n}\right| < \frac{1}{2bB_n}$$

ugr Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

Razonamos ahora por reducción al absurdo. Si $\frac{a}{b} \neq \frac{A_n}{B_n} \iff bA_n - aB_n \neq 0$, entonces $1 \leq |bA_n - aB_n|$ y obtenemos una contradicción ya que

$$\frac{1}{bB_n} \leq \frac{|bA_n - aB_n|}{bB_n} = \left|\frac{A_n}{B_n} - \frac{a}{b}\right| \leq \left|\alpha - \frac{A_n}{B_n}\right| + \left|\alpha - \frac{a}{b}\right| < \frac{1}{2bB_n} + \frac{1}{2b^2}$$

$$\Longrightarrow 1 < \frac{1}{2} + \frac{B_n}{2b} \iff \frac{1}{2} < \frac{B_n}{2b} \iff b < B_n \text{ Absurdo}$$

La única forma de salvar la contradicción es que $bA_n - aB_n = 0 \iff \frac{a}{b} = \frac{A_n}{B_n}$.
O sea, $\frac{a}{b}$ coincide con la n-convergente tal que $B_n \leq b < B_{n+1}$. □

Ahora podemos demostrar para todo $\rho, \sigma \in \mathbb{R}^+$ reales positivos que

Teorema 5. *Si $\sqrt{\rho}$ es irracional y $0 < \sigma < \sqrt{\rho}$. Toda solución positiva de la e.d. $x^2 - \rho y^2 = \sigma$ es una convergente de la FCS de $\sqrt{\rho}$.*

Demostración: Si $0 < a, b \in \mathbb{Z}$ son soluciones de $x^2 - \rho y^2 = \sigma$. Entonces,

$$\frac{a}{b} - \sqrt{\rho} = \frac{a - b\sqrt{\rho}}{b} = \frac{a^2 - \rho b^2}{b\left(a + b\sqrt{\rho}\right)} = \frac{\sigma}{b\left(a + b\sqrt{\rho}\right)} < \frac{\sqrt{\rho}}{b\left(a + b\sqrt{\rho}\right)} = \frac{1}{b^2\left(\frac{a}{b\sqrt{\rho}} + 1\right)}$$

La primeras igualdades nos dicen que $0 < \frac{a}{b} - \sqrt{\rho}$ y por tanto también

$$\sqrt{\rho} < \frac{a}{b} \iff 1 < \frac{a}{b\sqrt{\rho}} \Longrightarrow \frac{1}{b^2\left(\frac{a}{b\sqrt{\rho}} + 1\right)} < \frac{1}{2b^2}$$

ugr Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

Con las dos desigualdades obtenemos la hipótesis del teorema anterior

$$\left|\frac{a}{b} - \sqrt{\rho}\right| < \frac{1}{2b^2}$$

y por tanto a/b es una convergente de $\sqrt{\rho}$. $\square$

Particularizando a números enteros positivos, tenemos

Corolario 4. *Si $0 < d, N \in \mathbb{Z}$, d no cuadrado perfecto y $N < \sqrt{d}$. Toda solución positiva de $x^2 - dy^2 = N$ es una convergente de la FCS de $\sqrt{d}$.*

Si queremos resolver la misma e.d. con $N < 0$ y $|N| < \sqrt{d}$, hacemos

$$x^2 - dy^2 = N \Longleftrightarrow y^2 - \frac{1}{d}x^2 = -\frac{N}{d}$$

y aplicamos el teorema anterior para $\sigma = -N/d$ y $\rho = 1/d$. Como $0 < d$

$$0 < -N = |N| < \sqrt{d} \Longleftrightarrow 0 < -\frac{N}{d} < \frac{\sqrt{d}}{d} = \sqrt{\frac{1}{d}}$$

Por el teorema, sus soluciones positivas y, x son convergentes de $1/\sqrt{d}$. Pero si $\alpha = [q_0, q_1, \ldots]$ es la FCS de un α mayor que 1. Su inverso es menor que 1 y como $\frac{1}{\alpha} = 0 + \frac{1}{\alpha}$ su FCS empieza con cero y continua con la de α. O sea,

$$\frac{1}{\alpha} = [0, q_0, q_1, \ldots]$$

Además, si denotamos A_n, B_n y A'_n, B'_n los convergentes de α y $\frac{1}{\alpha}$ tenemos

$$\begin{array}{llll} A_0 = q_0, & A_1 = q_0 q_1 + 1, & & \dots, \quad A_n = q_{n-1} A_{n-1} + A_{n-2} \\ B_0 = 1, & B_1 = q_1, & & \dots, \quad B_n = q_{n-1} B_{n-1} + B_{n-2} \\ A'_0 = 0, & A'_1 = 1, & A'_2 = q_1, & \dots, \quad A'_n = q_{n-1} A'_{n-1} + A'_{n-2} \\ B'_0 = 1, & B'_1 = q_0, & B'_2 = q_0 q_1 + 1, & \dots, \quad B'_n = q_{n-1} B'_{n-1} + B'_{n-2} \end{array}$$

que $\frac{A_0}{B_0} = \frac{q_0}{1}$ y $\frac{A_1}{B_1} = \frac{q_0 q_1 + 1}{q_1}$ son los inversos de $\frac{A'_1}{B'_1} = \frac{1}{q_0}$ y que $\frac{A'_2}{B'_2} = \frac{q_1}{q_0 q_1 + 1}$. Como satisfacen las mismas ecuaciones en recurrencia con los q_i desplazados una unidad. Por inducción, esa relación es cierta para todo i. O sea,

Teorema 6. *Si $1 < \alpha \in \mathbb{R}$, la n-ésima convergente de $1/\alpha$ es la inversa de $n-1$-ésima convergente de α.*

Corolario 5. *Si $d, N \in \mathbb{Z}$, $0 < d$ no cuadrado perfecto y $N < 0$ con $|N| < \sqrt{d}$. Toda solución positiva de $x^2 - d y^2 = N$ es una convergente de la FCS de $\sqrt{d}$.*

Demostración: Por lo anterior, sus soluciones $0 < x, y \in \mathbb{Z}$ son soluciones de $y^2 - \frac{1}{d} x^2 = -\frac{N}{d}$ y estas $\frac{y}{x}$ son convergentes de $\frac{1}{\sqrt{d}}$ que a su vez son inversos de convergentes de $\sqrt{d}$. Luego $\frac{x}{y}$ es una convergente de $\sqrt{d}$ como queríamos.□

Ejemplo 17. *La FCS $\sqrt{61} = [7, \overline{1,4,3,1,2,2,1,3,4,1,14}]$ con convergentes*

$$\left\{7, 8, \frac{39}{5}, \frac{125}{16}, \frac{164}{21}, \frac{453}{58}, \frac{1070}{137}, \frac{1523}{195}, \frac{5639}{722}, \frac{24079}{3083}, \frac{29718}{3805}, \frac{440131}{56353}\right\}$$

da una solución a la e.d. ya que el tercero, $39^2 - 61 * 5^2 = -4$.

ugr Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

Página web personal
Página de Abertura
Contenido
◀◀ ▶▶
◀ ▶

Atrás
Pantalla grande/pequeña
Cerrar

Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

13. Ecuaciones cuadráticas diofánticas

Hemos visto que las e.d. $x^2 - dy^2 = \pm N$ con $|N| < \sqrt{d}$ y $d \in \mathbb{Z}^+$ no cuadrado perfecto si tienen soluciones positivas se encuentran entre los convergentes de la FCS de $\sqrt{d}$. De mostraremos que siempre existen soluciones positivas y que sus soluciones enteras están generadas por la más pequeña positiva.

Las e.d. $x^2 - dy^2 = \pm 1$ son importantes ya que sus soluciones corresponden a unidades del anillo $\mathbb{Z}\left[\sqrt{d}\right]$. Sus soluciones son un caso particular de las anteriores porque $x^2 - dy^2 = \pm 1 \Longrightarrow (2x)^2 - d(2y)^2 = \pm 4$.

En el caso $d \equiv 1 \pmod 4$, las e.d. $x^2 - dy^2 = \pm 4$ son importantes porque sus soluciones corresponden a unidades del anillo de enteros del c.c. $Q(\sqrt{d})$:

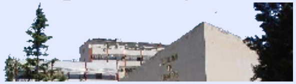
$$\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{\frac{a+b\sqrt{d}}{2} : \ a, b \in \mathbb{Z}, \ a \equiv b \pmod 2\right\}$$

La norma de un e.a. de este anillo vale ± 1 cuando son soluciones de la e.d.

$$N\left(\frac{a+b\sqrt{d}}{2}\right) = \left(\frac{a+b\sqrt{d}}{2}\right)\left(\frac{a-b\sqrt{d}}{2}\right) = \frac{a^2-db^2}{4} = \pm 1 \Longleftrightarrow a^2 - db^2 = \pm 4$$
$$U\left(\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]\right) = \left\{\frac{a+b\sqrt{d}}{2} : \ a^2 - db^2 = \pm 4, \ a \equiv b \pmod 2\right\}$$

Observamos que $\mathbb{Z}\left[\sqrt{d}\right] \subset \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ y que las unidades de $\mathbb{Z}[\sqrt{d}]$ son un caso particular de las unidades de $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, cuando a, b son ambos pares.

Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra



Teorema 7. *Si* $0 < a, b \in \mathbb{Z}$ *son las menores soluciones de* $x^2 - dy^2 = \pm 4$, *con* $0 < d \equiv 1 \pmod 4$ *no cuadrado perfecto. Entonces todas sus soluciones enteras* $s, t \in \mathbb{Z}$ *se obtienen de* $\pm\left(\frac{a+b\sqrt{d}}{2}\right)^n = \frac{s+t\sqrt{d}}{2}$ *con* $n \in \mathbb{Z}$.

Demostración: Basta con que las soluciones positivas se obtengan como $\left(\frac{a+b\sqrt{d}}{2}\right)^n = \frac{s+t\sqrt{d}}{2}$ con $n \in \mathbb{N}$ ya que si $s^2 - dt^2 = \pm 4$ entonces también son soluciones $\pm s, \pm t \in \mathbb{Z}$. O sea, hay 4 soluciones que corresponden a los e.a.

$$\frac{s+t\sqrt{d}}{2}, \frac{-s-t\sqrt{d}}{2}, \frac{s-t\sqrt{d}}{2}, \frac{-s+t\sqrt{d}}{2}$$

que son opuestos dos a dos,. Los exponentes negativos se obtienen ya que

$$\left(\frac{s+t\sqrt{d}}{2}\right)^{-1} = \begin{cases} \frac{s-t\sqrt{d}}{2} & \text{Si } s^2 - dt^2 = 4 \\ \frac{-s+t\sqrt{d}}{2} & \text{Si } s^2 - dt^2 = -4 \end{cases}$$

Ahora, si $0 < a, b \in \mathbb{Z}$ son las menores soluciones, $\alpha = \frac{a+b\sqrt{d}}{2}$ es un e.a. porque su polmin, $x^2 - ax + \frac{a^2-db^2}{4} = x^2 - ax \pm 1 \in \mathbb{Z}[x]$, es entero. Y como tiene norma ± 1, es una unidad del anillo $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Luego cualquier potencia positiva suya también lo es y por tanto es de la forma. $\alpha^n = \frac{a_n+b_n\sqrt{d}}{2}$. Luego $0 < a_n, b_n \in \mathbb{Z}$ son soluciones de $x^2 - dy^2 = \pm 4$ y $a_n \equiv b_n \pmod 2$.

Recíprocamente, si $0 < s, t \in \mathbb{Z}$ son soluciones de la e.d. $x^2 - dy^2 = \pm 4$, $\beta = \frac{s+t\sqrt{d}}{2}$ igual que $\alpha = \frac{a+b\sqrt{d}}{2}$ es un número real mayor que 1[1].
Y como $\mathbb{R}$ es arquimediano, existe un natural $m \in \mathbb{N}$ tal que

$$\alpha^m \leq \beta < \alpha^{m+1} \Longrightarrow 1 \leq \beta\alpha^{-m} < \alpha$$

ya que $0 < \alpha^{-1} \Leftrightarrow 0 < \alpha^{-m}$ son reales positivos porque $\alpha\alpha^{-1} = 1$.

Ahora, $\beta\alpha^{-m}$, como producto de unidades es una unidad del a.e. $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.
Por tanto de la forma $\beta\alpha^{-m} = \frac{a'+b'\sqrt{d}}{2}$ con $a'^2 - db'^2 = \pm 4$.

Basta comprobar que $0 < a', b'$ son enteros positivos para que la minimalidad de α implique que $\beta\alpha^{-m} = 1$ y $\beta = \alpha^m$ como queríamos demostrar. Pero

$$\left(\frac{a'+b'\sqrt{d}}{2}\right)^{-1} = \begin{cases} \frac{a'-b'\sqrt{d}}{2} & \text{Si } a'^2 - db'^2 = 4 \\ \frac{-a'+b'\sqrt{d}}{2} & \text{Si } a'^2 - db'^2 = -4 \end{cases}$$

Si $1 < \beta\alpha^{-m}$ su inverso satisface $0 < \left(\frac{a'+b'\sqrt{d}}{2}\right)^{-1} < 1$ y tenemos

$$\begin{cases} 0 < a' = \frac{a'+b'\sqrt{d}}{2} + \frac{a'-b'\sqrt{d}}{2} & \text{Si } a'^2 - db'^2 = 4 \\ 0 < b'\sqrt{d} = \frac{a'+b'\sqrt{d}}{2} - \frac{a'-b'\sqrt{d}}{2} & \text{Si } a'^2 - db'^2 = 4 \\ 0 < b'\sqrt{d} = \frac{a'+b'\sqrt{d}}{2} + \frac{-a'+b'\sqrt{d}}{2} & \text{Si } a'^2 - db'^2 = -4 \\ 0 < a' = \frac{a'+b'\sqrt{d}}{2} - \frac{-a'+b'\sqrt{d}}{2} & \text{Si } a'^2 - db'^2 = -4 \end{cases}$$

[1] $0 < d \equiv 1 \ (4)$ y por tanto $d \geq 5$.

ugr Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

Veremos que siempre existe una menor solución con a y b positivos de la e.d. $x^2 - dy^2 = \pm 1$ y por tanto también existe una de $(2x)^2 - d(2y)^2 = \pm 4$ y su menor positiva. Por tanto, si $0 < d \equiv 1 \pmod 4$ no cuadrado perfecto,

Corolario 6. *El conjunto de soluciones de $x^2 - dy^2 = \pm 4$ tiene estructura de grupo abeliano isomorfo a $\mathbb{Z}_2 \oplus \mathbb{Z}$.*

Como los únicos elementos de orden finito entre las soluciones corresponden a $\alpha = \frac{\pm 2 + 0\sqrt{d}}{2} = \pm 1$, el resto generan subgrupos isomorfos a $\mathbb{Z}$. Por tanto,

Corolario 7. *El conjunto de las soluciones de $x^2 - dy^2 = \pm 1$ tiene estructura de grupo abeliano isomorfo a $\mathbb{Z}_2 \oplus \mathbb{Z}$.*

Definición 1. *Decimos **solución positiva s.p.** si $0 < a, b \in \mathbb{Z}$ y **solución fundamental SF** si $\alpha = \frac{a + b\sqrt{d}}{2}$ no es una potencia de otro i.c.*

Como las soluciones van de 4 en 4, $\pm a, \pm b$. Hay 4 soluciones fundamentales de las cuales sólo una es positiva. Pero si se consideran los e.a. correspondientes hay dos positivos: $\alpha = \frac{a + b\sqrt{d}}{2}$ con $0 < a, b$ y su inverso α^{-1}.

Aunque las soluciones de $x^2 - dy^2 = \pm 1$ están contenidas entre las de $x^2 - dy^2 = \pm 4$, a veces coinciden. Por ejemplo,

Ejemplo 18. *La FCS $\sqrt{17} = [4, \overline{8}]$ sólo tiene 1 convergente $\frac{4}{1}$ que corresponde al e.a. $\alpha = 4 + \sqrt{17}$ y SF $a = 4,\ b = 1$ de $x^2 - dy^2 = -1$ o bien $a = 8,\ b = 4$ que es la SF positiva de $x^2 - dy^2 = -4$.*

ugr Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

14. Caracterización de FCS periódicas

Recordamos que una FCS $\alpha = [q_0, q_1 \dots]$ se dice **periódica** si existen $n, r \in \mathbb{N}$ tal que $q_r = q_{n+r}$. Si n, r son mínimos la FCS se escribe como

$$[q_0, \dots, q_{r-1}, \overline{q_r, \dots, q_{n+r}}] \text{ o bien } [q_0, \dots, q_{r-1}, \overline{a_0, \dots, a_{n-1}}]$$

para indicar el periodo $a_0, \dots, a_{n-1}$ que se repite indefinidamente.

Hemos visto en una sección anterior que la FCS de un irracional cuadrático es periódica con periodo como máximo $2d-1$. También es cierto el recíproco.

Teorema 8. *Una FCS es periódica si y sólo si es la de un i.c.*

Demostración: Queda por demostrar la condición necesaria: Supongamos $\alpha = [q_0, \dots, q_{r-1}, \overline{a_0, \dots, a_{n-1}}]$ y $\theta = [\overline{a_0, \dots, a_{n-1}}]$ su parte periódica. Como las dos FC son infinitas, ambos números reales α, θ no pueden ser racionales.

Por el lema 1, para todo $x \in \mathbb{R}$, se tiene $[q_0, q_1, q_2, \dots, q_r, x] = \frac{xA_r + A_{r-1}}{xB_r + B_{r-1}}$. Así

$$\alpha = [q_0, \dots, q_{r-1}, \theta] \Longrightarrow \alpha = \frac{\theta A_{r-1} + A_{r-2}}{\theta B_{r-1} + B_{r-2}}$$
$$\theta = [\overline{a_0, \dots, a_{n-1}}] = [a_0, \dots, a_{n-1}, \theta] \Longrightarrow \theta = \frac{\theta A'_{n-1} + A'_{n-2}}{\theta B'_{n-1} + B'_{n-2}}$$

Pero la 2ª igualdad equivale a una ecuación cuadrática con coeficientes enteros en θ igualada a cero. Que nos dice que θ es un i.c. Si lo sustituimos en la 1ª igualdad, nos dice que α también es i.c. como queríamos. □

Definición 2. *Una FCS se dice* ***puramente periódica*** *si es de la forma* $[\overline{a_0,\ldots,a_{n-1}}]$.

Ejemplo 19. $\alpha = \frac{1+\sqrt{3}}{2}$ *está en forma normal, el algoritmo termina y la FCS*

$$\left.\begin{array}{llll} Paso & 0 & 1 & 2 \\ P_i & 1 & 1 & 1 \\ Q_i & 2 & 1 & 2 \\ q_i & 1 & 2 & 1 \end{array}\right\} \Longrightarrow \alpha = \frac{1+\sqrt{3}}{2} = \alpha_2 \Longrightarrow \alpha = [\overline{1,2}]$$

es puramente periódica con periodo de longitud 2.

Teorema 9. *Un i.c.* α *es puramente periódico si y sólamente si* $1 < \alpha = \frac{a+\sqrt{b}}{c}$ *y su conjugado* $\overline{\alpha} = \frac{a-\sqrt{b}}{c}$ *satisface* $-1 < \overline{\alpha} < 0$.

Demostración: Primero suponemos que α es p.p. Por tanto,

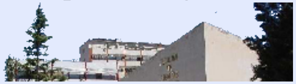
$$\alpha = [a_0,\ldots,a_{n-1},\alpha] = \frac{\alpha A_{n-1} + A_{n-2}}{\alpha B_{n-1} + B_{n-2}} \Longrightarrow \alpha^2 B_{n-1} + \alpha(B_{n-2} - A_{n-1}) - A_{n-2} = 0$$

O sea, α es raíz de $F(x) = x^2 B_{n-1} + x(B_{n-2} - A_{n-1}) - A_{n-2} \in \mathbb{Z}[x]$, polinomio que tiene dos raíces una es α y la otra es su conjugado $\overline{\alpha}$.

Como α es p.p. todos los q_i son enteros positivos. Por tanto, $1 \le q_0 < \alpha$.
Y la otra raíz está en $(-1,0)$ ya que $f(0) = -A_{n-2} < 0$ y

$$\begin{aligned} f(-1) &= B_{n-1} - B_{n-2} + A_{n-1} - A_{n-2} = \\ &= B_{n-2} q_{n-1} + B_{n-3} + A_{n-2} q_{n-1} + A_{n-3} - B_{n-2} - A_{n-2} = \\ &= (B_{n-2} + A_{n-2})(q_{n-1} - 1) + B_{n-3} + A_{n-3} > B_{n-3} + A_{n-3} > 0 \end{aligned}$$

Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra



Recíprocamente, supongamos que $1 < \alpha$ y $-1 < \overline{\alpha} < 0$. Entonces

$$\alpha_i = q_i + \frac{1}{\alpha_{i+1}} \iff \frac{1}{\overline{\alpha_{i+1}}} = \overline{\alpha_i} - q_i$$

Como $1 < \alpha \Longrightarrow 1 \leq q_0$. Por tanto, $1 \leq q_i$, para todo $i \geq 0$. Entonces,

$$\text{Si } \overline{\alpha_i} < 0 \Longrightarrow \frac{1}{\overline{\alpha_{i+1}}} < -1 \iff -1 < \overline{\alpha_{i+1}} < 0$$

Por hipótesis, $-1 < \overline{\alpha_0} < 0$. Entonces, por inducción, $-1 < \overline{\alpha_i} < 0,\ \forall i \geq 0$.
Y multiplicando por -1 cambian esas desigualdades. O sea, tenemos

$$0 < -\overline{\alpha_i} = -\frac{1}{\alpha_{i+1}} - q_i < 1 \Longrightarrow q_i = \left[-\frac{1}{\alpha_{i+1}}\right]$$

Como α es i.c. su FCS es periódica y existen $0 < j < k$ tales que $\alpha_j = \alpha_k$.
Conjugando tenemos $\overline{\alpha_j} = \overline{\alpha_k}$ y por tanto

$$q_{j-1} = \left[-\frac{1}{\alpha_j}\right] = \left[-\frac{1}{\alpha_k}\right] = q_{k-1} \Longrightarrow \alpha_{j-1} = q_{j-1} + \frac{1}{\alpha_j} = q_{k-1} + \frac{1}{\alpha_k} = \alpha_{k-1}$$

Por inducción finita hacia abajo, tenemos $\alpha_j = \alpha_k \Longrightarrow \alpha_0 = \alpha_{k-j}$.
O sea, $\alpha = \alpha_0 = [\overline{q_0, \ldots, q_{k-j-1}}]$ es p.p. como queríamos. □

Corolario 8. *Si $\alpha = [\overline{q_0, \ldots, q_{r-1}}]$ es p.p. Entonces, $-1/\overline{\alpha} = [\overline{q_{r-1}, \ldots, q_0}]$.*

Demostración:$-1 < \overline{\alpha} \iff 1 < -1/\overline{\alpha}$ y también $1 < \alpha \iff -1 < -1/\alpha < 0$
$\alpha = \alpha_0 = q_0 + \frac{1}{\alpha_1}, \ldots, \alpha_{r-1} = q_{r-1} + \frac{1}{\alpha_0} \Longrightarrow \overline{\alpha_0} = q_0 + \frac{1}{\overline{\alpha_1}}, \ldots, \overline{\alpha_{r-1}} = q_{r-1} + \frac{1}{\overline{\alpha_0}}$

ugr Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

Y despejando de atrás adelante $-\frac{1}{\alpha_0} = q_{r-1} - \overline{\alpha_{r-1}} \ldots, -\frac{1}{\alpha_1} = q_0 - \alpha_0$ se obtienen los cocientes en el orden inverso como queremos. $\square$

Para $\sqrt{d}$, con $0 < d$ entero no cuadrado perfecto, siempre $-\sqrt{d} < -1$. Sin embargo, el i.c. asociado $\sqrt{d} + \left[\sqrt{d}\right]$ satisface $-1 < -\sqrt{d} + \left[\sqrt{d}\right] < 0$. O sea,

Corolario 9. *$\sqrt{d}$ nunca es p.p. pero si lo es $\sqrt{d} + \left[\sqrt{d}\right]$.* $\square$

Por tanto, $\alpha = \sqrt{d} + \left[\sqrt{d}\right] = [\overline{q_0, \ldots, q_{r-1}}]$ donde r es la longitud del periodo. Así, $\alpha = [q_0, \ldots, q_{i-1}, \alpha_i]$ donde $\alpha_i = [\overline{q_i, \ldots, q_{r-i}}]$ es p.p. para cada $i \in \mathbb{N}$. Además, $\alpha, \alpha_1, \ldots, \alpha_{r-1}$ son todos diferentes entre si y $\alpha = \alpha_r = \alpha_{2r} = \cdots$

$$\alpha = \sqrt{d} + \left[\sqrt{d}\right] = [\overline{q_0, \ldots, q_{r-1}}] = [q_0, \ldots, q_{i-1}, \overline{q_i, \ldots, q_{r-i}}]$$

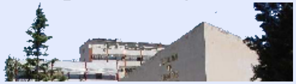
Los i.c. $\alpha_i = [\overline{q_i, \ldots, q_{r-i}}]$ son necesariamente de la forma $\frac{P_i + \sqrt{d}}{Q_i}$ y satisfacen

$$\frac{P_{jr} + \sqrt{d}}{Q_{jr}} = \alpha_{jr} = \alpha = \left[\sqrt{d}\right] + \sqrt{d} \Longleftrightarrow P_{jr} - Q_{jr}\left[\sqrt{d}\right] = (Q_{jr} - 1)\sqrt{d}$$

Como $\sqrt{d}$ es irracional la igualdad debe ser cero. Pero sólo en estos casos, ya que si $Q_i = 1$ y $\alpha_i = P_i + \sqrt{d}$ como es p.p. su conjugado debe satisfacer

$$-1 < P_i - \sqrt{d} < 0 \Longleftrightarrow \sqrt{d} - 1 < P_i < \sqrt{d} \Longrightarrow P_i = \left[\sqrt{d}\right] \Longrightarrow \alpha_i = \alpha$$

Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra



O sea, $Q_{jr} = 1$ para todo $j \in \mathbb{N}$ y $Q_i \neq 1$ para todo $i = 1, \dots, r-1$.
Además, $Q_i \neq -1$ para todo $i \in \mathbb{N}$. Ya que si $P_i = -1$, el i.c. $\alpha_i = -P_i - \sqrt{d}$ como es p.p. debe ser mayor que 1 y su conjugado estar entre 0 y 1.

$$\left.\begin{array}{l} 1 < -P_i - \sqrt{d} \Longrightarrow P_i < -1 - \sqrt{d} \\ -1 < -P_i + \sqrt{d} < 0 \Longrightarrow \sqrt{d} < P_i \end{array}\right\} \Longrightarrow \sqrt{d} < P_i < -1 - \sqrt{d} \text{ Absurdo}$$

Ahora, estamos en condiciones de caracterizar la FCS de $\sqrt{d}$ comparándola con la de $\alpha = \sqrt{d} + [\sqrt{d}]$. Así, si $0 < d \in \mathbb{Z}$ no cuadrado perfecto,

Teorema 10. *$\sqrt{d} = [a_0, \overline{a_1, a_2, \dots, a_{r-1}, 2a_0}]$ y $a_1, a_2, \dots, a_{r-1}$ es simétrico respecto de su centro. Y $Q_i = 1$ si y sólamente si $r | i$ y $Q_i \neq -1$ para todo i.*

Demostración: Observamos que en la FCS de $\sqrt{d} + [\sqrt{d}]$ la primera parte entera es $q_0 = [\alpha] = \left[\sqrt{d} + [\sqrt{d}]\right] = 2[\sqrt{d}]$ y entonces

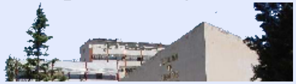
$$\sqrt{d} = -[\sqrt{d}] + (\sqrt{d} + [\sqrt{d}]) = -[\sqrt{d}] + [q_0, \overline{q_1, q_2, \dots, q_{r-1}, q_0}] =$$
$$= -[\sqrt{d}] + \left[2[\sqrt{d}], \overline{q_1, q_2, \dots, q_{r-1}, q_0}\right] = \left[[\sqrt{d}], \overline{q_1, q_2, \dots, q_{r-1}, 2[\sqrt{d}]}\right]$$

Por tanto, la FCS de $\sqrt{d}$ coincide con la de $\sqrt{d} + [\sqrt{d}]$ a partir de la segunda iteración. Por el cor 8, como $\alpha_1 = \frac{1}{\sqrt{d} - [\sqrt{d}]} = [\overline{q_1, q_2, \dots, q_{r-1}, q_0}]$ es p.p.

$$-1/\overline{\alpha_1} = [\overline{q_0, q_{r-1}, \dots, q_2, q_1}] = \sqrt{d} + [\sqrt{d}] = [\overline{q_0, q_2, \dots, q_{r-1}}]$$

de donde se obtiene la simetría y todo está demostrado. $\square$

ugr Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra



El que los denominadores de los $\alpha_i = \frac{P_i+\sqrt{d}}{Q_i}$ nunca valen -1 y sólo valen 1 en los múltiplos de la longitud del periodo permite hallar las soluciones de

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

En efecto, por el lema 1, $\sqrt{d} = [q_0, \dots, q_n, \alpha_{n+1}] = \frac{\alpha_{n+1}A_n + A_{n-1}}{\alpha_{n+1}B_n + B_{n-1}}$ y entonces

$$\sqrt{d} = \frac{\alpha_{n+1}A_n + A_{n-1}}{\alpha_{n+1}B_n + B_{n-1}} = \frac{(P_{n+1}+\sqrt{d})A_n + Q_{n+1}A_{n-1}}{(P_{n+1}+\sqrt{d})B_n + Q_{n+1}B_{n-1}} = \frac{P_{n+1}A_n + Q_{n+1}A_{n-1} + \sqrt{d}A_n}{P_{n+1}B_n + Q_{n+1}B_{n-1} + \sqrt{d}B_n}$$
$$\Longrightarrow dB_n + (P_{n+1}B_n + Q_{n+1}B_{n-1})\sqrt{d} = P_{n+1}A_n + Q_{n+1}A_{n-1} + \sqrt{d}A_n$$

como $\sqrt{d}$ es irracional, deben ser iguales sus coeficientes. Por tanto,

$$\left.\begin{array}{r} A_n = P_{n+1}B_n + Q_{n+1}B_{n-1} \\ dB_n = P_{n+1}A_n + Q_{n+1}A_{n-1} \end{array}\right\} \Longrightarrow \left.\begin{array}{r} A_n^2 = P_{n+1}A_nB_n + Q_{n+1}A_nB_{n-1} \\ dB_n^2 = P_{n+1}A_nB_n + Q_{n+1}A_{n-1}B_n \end{array}\right\} \Longrightarrow$$
$$\Longrightarrow A_n^2 - dB_n^2 = (A_{n-1}B_n - A_nB_{n-1})Q_{n+1} = (-1)^{n-1}Q_{n+1}$$

O sea, si $0 < d \in \mathbb{Z}$, no es cuadrado perfecto, hemos demostrado que

Teorema 11. $A_{n-1}^2 - dB_{n-1}^2 = (-1)^n Q_n$ *para todo entero* $n \geq 0$.

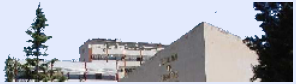
Esta propiedad, da una forma de resolver la **ecuación de Pell**, $x^2 - dy^2 = \pm 1$[2].

Corolario 10. *Las soluciones positivas de* $x^2 - dy^2 = \pm 1$ *son los convergentes* A_{n-1}, B_{n-1} *de* $\sqrt{d}$ *con* n *un múltiplo de* r *la longitud del periodo.*

---

[2] Ya que sabemos que $Q_i = 1$ si y sólamente si $r|i$ donde r es la longitud del periodo de la descomposición en FCS de $\sqrt{d}$ y Q_i nunca vale -1.

ugr Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra



Así, el algoritmo de FCS de $\sqrt{d}$ termina cuando detectemos el primer $Q_r = 1$ después del inicial, equivalentemente la primera vez que $q_i = 2q_0$.

La convergente anterior A_{r-1}, B_{r-1} es la menor s.p. de la ecuación de Pell y $A_{r-1} + B_{r-1}\sqrt{d}$ es su SF . Además, por el cor 7, tenemos

Teorema 12. *Si $A_{r-1}, B_{r-1} \in \mathbb{N}$ es la menor s.p. de $x^2 - dy^2 = \pm 1$, sus soluciones se obtienen de la igualdad $x_n + y_n\sqrt{d} = \pm(A_{r-1} + B_{r-1}\sqrt{d})^n$ con $n \in \mathbb{Z}$.*

Por lo anterior, también es posible resolver la e.d. $x^2 - dy^2 = \pm 4$ que es una forma de calcular una unidad fundamental del a.e. del c.c. $\mathbb{Q}(\sqrt{d})$. En efecto:

Como la menor s.p. de $x^2 - dy^2 = \pm 1$ nos da una s.p. $(2x_1)^2 - d(2y_1)^2 = \pm 4$, tiene que existir la menor s.p. de $x^2 - dy^2 = \pm 4$. Y por el cor 4, tenemos que encontrarla entre los convergentes de $\sqrt{d}$ anteriores o iguales a A_{r-1}, B_{r-1}.

Teorema 13. *La menor s.p. de $x^2 - dy^2 = \pm 4$ es la primera convergente A_i, B_i de $\sqrt{d}$ que corresponde a $\alpha_i = \frac{P_i + \sqrt{d}}{Q_i}$ cuyo denominador sea $Q_i = 4$. Si no existe ese denominador, la menor s.p. es $2A_{r-1}, 2B_{r-1}$.*

Demostración: Basta aplicar $A_{i-1}^2 - dB_{i-1}^2 = (-1)^i Q_i$ para $0 \leq n \leq r-1$. $\square$

Corolario 11. *Si $d \equiv 1 \pmod 4$, una unidad fundamental del a.e. de $\mathbb{Q}(\sqrt{d})$ es $\frac{a+b\sqrt{d}}{2}$ donde $0 < a, b \in \mathbb{Z}$ es la menor s.p. de $x^2 - dy^2 = \pm 4$.*

Ejemplo 20. *Para $\mathbb{Q}(\sqrt{17})$ una unidad fundamental es $\alpha = \frac{8+2\sqrt{17}}{2} = 4 + \sqrt{17}$.*

Página web personal
Página de Abertura
Contenido
Página 36 de 44
Atrás
Pantalla grande/pequeña
Cerrar

15. Aplicaciones

$\sqrt{d}$ siempre está en forma normal porque $Q_0 = 1$, también $P_0 = 0$ y $q_0 = \lfloor \sqrt{d} \rfloor$ y se le puede aplicar el algoritmo de cálculo.

En general, si $\alpha = \frac{P_0+\sqrt{d}}{Q_0}$ es un i.c. con $Q_0|(d-P_0^2)$ el algoritmo de cálculo de su FCS sucesivamente calcula los $\alpha_i = \frac{P_1+\sqrt{d}}{Q_i}$ así:

$$\begin{array}{ccc}
q_0 = \lfloor\alpha\rfloor = Quot(P_0 + \lfloor\sqrt{d}\rfloor, Q_0), & P_1 = q_0Q_0 - P_0, & Q_1 = \frac{d-P_0^2}{Q_0} \\
q_1 = \lfloor\alpha_1\rfloor = Quot(P_1 + \lfloor\sqrt{d}\rfloor, Q_1), & P_2 = q_1Q_1 - P_1, & Q_2 = Q_0 + q_1(P_1 - P_2) \\
\vdots & \vdots & \vdots \\
q_i = \lfloor\alpha_i\rfloor = Quot(P_i + \lfloor\sqrt{d}\rfloor, Q_i), & P_{i+1} = q_iQ_i - P_i, & Q_{i+1} = Q_{i-2} + q_i(P_i - P_{i+1})
\end{array}$$

Y en cada iteración, se calculan también los convergentes con las e.r.

$$\begin{array}{ll}
A_i = q_iA_{i-1} + A_{i-2}, & A_{-1} = 1, A_0 = q_0 \\
B_i = q_iB_{i-1} + B_{i-2}, & B_{-1} = 0, B_0 = 1
\end{array}$$

En cada iteración se comprueba si $Q_i = 4$, en cuyo caso se guarda el anterior i.c. $\frac{A_{i-1}+B_{i-1}\sqrt{d}}{2}$. El primero da la UF positiva del c.c. $\mathbb{Q}(\sqrt{d})$.

Si no se encuentra ningún 4, se termina el algoritmo con el primer $Q_r = 1$ y se devuelve $A_{r-1} + B_{r-1}\sqrt{d}$ que es la UF positiva en este caso.

ugr Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

Ejemplo 21. *La FCS* $\sqrt{21} = [4, \overline{1,1,2,1,1,8}]$ *con periodo de longitud 6, cuyos e.a y convergentes que dan solución a* $x^2 - dy^2 = \pm 4$ *son*

$$\left\{\frac{4+\sqrt{21}}{5}, \frac{1+\sqrt{21}}{4}, \frac{3+\sqrt{21}}{3}, \frac{3+\sqrt{21}}{4}, \frac{1+\sqrt{21}}{5}, 4+\sqrt{21}\right\}$$
$$\left\{4, 5, \frac{9}{2}, \frac{23}{5}, \frac{32}{7}, \frac{55}{12}\right\}$$

En este caso, no hay solución a $x^2 - 21y^2 = -4$ *porque la iteración es par. La primera la da el 2º convergente ya que* $5^2 - 21 * 1^2 = 4$. *Por tanto corresponde a la UF* $\alpha = \frac{5+\sqrt{21}}{2}$ *de* $\mathbb{Q}(\sqrt{21})$ *porque* $21 \equiv 1 \pmod 4$. *Los siguientes son*

$$\alpha^2 = \left(\frac{5+\sqrt{21}}{2}\right)^2 = \frac{23+5\sqrt{21}}{2} \implies 23^2 - 21 * 5^2 = 4$$
$$\alpha^3 = \left(\frac{5+\sqrt{21}}{2}\right)^3 = 55 + 12\sqrt{21} \implies 55^2 - 21 * 12^2 = 1$$

Ejemplo 22. *La FCS* $\sqrt{29} = [5, \overline{2,1,1,2,10}]$ *con periodo de longitud 5, cuyos e.a y convergentes que dan solución a* $x^2 - dy^2 = \pm 4$ *son*

$$\left\{\frac{5+\sqrt{29}}{4}, \frac{3+\sqrt{29}}{5}, \frac{2+\sqrt{29}}{5}, \frac{3+\sqrt{29}}{4}, 5+\sqrt{29}\right\}$$
$$\left\{5, \frac{11}{2}, \frac{16}{3}, \frac{27}{5}, \frac{70}{13}\right\}$$

Hay solución con -4 *porque la iteración es impar. Es el 1º convergente,* $5^2 - 29 * 1^2 = -4$. *Corresponde a la UF* $\alpha = \frac{5+\sqrt{29}}{2}$ *porque* $29 \equiv 1 \pmod 4$.

$$\alpha^2 = \left(\frac{5+\sqrt{29}}{2}\right)^2 = \frac{27+5\sqrt{29}}{2} \implies 27^2 - 29 * 5^2 = 4$$
$$\alpha^3 = \left(\frac{5+\sqrt{29}}{2}\right)^3 = 70 + 13\sqrt{21} \implies 70^2 - 29 * 13^2 = -1$$

Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

ugr Universidad de Granada

Enrique R. Aznar
Dpto. de Álgebra

Ejemplo 23. *La FCS* $\sqrt{61} = [7, \overline{1,4,3,1,2,2,1,3,4,1,14}]$ *con periodo de longitud 11, cuyos e.a y convergentes que dan solución a* $x^2 - dy^2 = \pm 4$ *son*

$$\left\{\frac{7+\sqrt{61}}{12}, \frac{5+\sqrt{61}}{3}, \frac{7+\sqrt{61}}{4}, \frac{5+\sqrt{61}}{9}, \frac{4+\sqrt{61}}{5}, \frac{6+\sqrt{61}}{5}, \frac{4+\sqrt{61}}{9}, \frac{5+\sqrt{61}}{4}, \frac{7+\sqrt{61}}{3}, \frac{5+\sqrt{61}}{12}, 7+\sqrt{61}\right\}$$
$$\left\{7, 8, \frac{39}{5}, \frac{125}{16}, \frac{164}{21}, \frac{453}{58}, \frac{1070}{137}, \frac{1523}{195}, \frac{5639}{722}, \frac{24079}{3083}, \frac{29718}{3805}\right\}$$

La primera la da el 3º convergente, $39^2 - 61 * 5^2 = -4$. *Corresponde a la UF* $\alpha = \frac{39+5\sqrt{61}}{2}$. *Hay solución con* -4 *porque la iteración es impar. Otras son*

$$\alpha^2 = \left(\frac{39+5\sqrt{61}}{2}\right)^2 = \frac{1523+195\sqrt{61}}{2} \implies 1523^2 - 61 * 195^2 = 4$$
$$\alpha^3 = \left(\frac{39+5\sqrt{61}}{2}\right)^3 = 29718 + 3805\sqrt{61} \implies 4\left(29718^2 - 61 * 3805^2\right) = -4$$

Ejemplo 24. *La FCS* $\sqrt{73} = [8, \overline{1,1,5,5,1,1,16}]$ *con periodo de longitud 7, cuyos e.a y convergentes que dan solución a* $x^2 - dy^2 = \pm 4$ *son*

$$\left\{\frac{8+\sqrt{73}}{9}, \frac{1+\sqrt{73}}{8}, \frac{7+\sqrt{73}}{3}, \frac{8+\sqrt{73}}{3}, \frac{7+\sqrt{73}}{8}, \frac{1+\sqrt{73}}{9}, 8+\sqrt{73}\right\}$$
$$\left\{8, 9, \frac{17}{2}, \frac{94}{11}, \frac{487}{57}, \frac{581}{68}, \frac{1068}{125}\right\}$$

La primera la da el 7º convergente, $1068^2 - 73 * 125^2 = -1$. *Hay solución con* -4 *porque la iteración es impar. Como no se ha encontrado ningún denominador* $Q_i = 4$ *antes del final del periodo. La UF es* $\alpha = 1068 + 125\sqrt{73}$.

En este caso, las unidades de $\mathbb{Z}[\sqrt{73}]$ *coinciden con las del a.e.* $\mathbb{Z}[\frac{1+\sqrt{73}}{2}]$. *O sea, las unidades de ambos anillos son*

$$\pm(1068 + 125\sqrt{73})^n, \text{ tal que } n \in \mathbb{Z}$$

Página web personal
Página de Abertura
Contenido
◀◀ ▶▶
◀ ▶
Página 39 de 44
Atrás
Pantalla grande/pequeña
Cerrar

16. Ejercicios.

Ejercicio 1. *Encuentra la longitud* r *del periodo de FCS de* $\sqrt{13290059}$ *y las unidades del anillo de enteros correspondiente.*

17. Referencias.

[1] David Bressoud, Stan Wagon: *A Course in Computational Number Theory*, John Wiley & Sons, Hoboken, NJ, USA, 2000.

[2] William B. Jones and W. J. Thron, Continued Fractions, Analytical Theory and Applications, Addison-Wesley, London, 1980.

[3] A. Ya. Khintchine, Continued Fractions, P. Noordhoff, Groningen, 1963.

[4] Niven I., Zuckerman H.S., An introduction to the theory of numbers, John Wiley & Sons, NY, 1972.

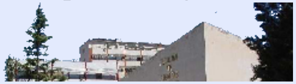
[5] Hans Riesel: *Prime Numbers and Computer Methods for Factorization*, Springer Science+Business Media, LLC 2012, (first edition Birkhäuser, 1994).

[6] Samuel S. Wagstaff, Jr: *The joy of factoring*, AMS, Providence, Rhode island, 2013.

18. Test de repaso.

Para comenzar el cuestionario pulsa el botón de inicio.
Cuando termines pulsa el botón de finalizar.

Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra



Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra

Para marcar una respuesta coloca el ratón en la letra correspondiente y pulsa el botón de la izquierda (del ratón).

Inicio del Test

1. Si $\alpha = \sqrt{2} \in \mathbb{R}$, su FCS es.

(a) $\alpha = [1, 1, 1, 1, \ldots]$
(b) $\alpha = [2, 2, 2, 2, \ldots]$
(c) No es periódica.
(d) $\alpha = [1, 2, 2, \ldots]$

2. Si $\alpha = \sqrt{3} \in \mathbb{R}$, su FCS es.

(a) $\alpha = [3, 3, 3, 3, \ldots]$
(b) $\alpha = [1, \overline{1, 3}, \overline{1, 3}, \ldots]$
(c) $\alpha = [\overline{1, 3}, \overline{1, 3}, \ldots]$
(d) No es puramente periódica.

3. Si $\alpha = \frac{a+\sqrt{a^2+4}}{2} \in \mathbb{R}$, su FCS es.

(a) $\alpha = [1, a, a, a, \ldots]$
(b) $\alpha = [2, a, a, a, \ldots]$
(c) No es periódica.

(d) $\alpha = [a, a, a, \ldots]$

4. Si $\alpha = \frac{1+\sqrt{5}}{2} \in \mathbb{R}$, su FCS es.

(a) $\alpha = [1, \overline{1,2}, \overline{1,2}, \ldots]$

(b) $\alpha = [2, 2, 2, \ldots]$

(c) $\alpha = [5, 5, 5, \ldots]$.

(d) $\alpha = [1, 1, 1, \ldots]$

5. ¿Cuál de las siguientes afirmaciones es verdadera?.

(a) $\sqrt{a^2-2} = [a-2, \overline{1, a-2, 1, 2(a-1)}, \ldots]$

(b) $\sqrt{a^2+2} = [a+1, a, 2a, a, 2a, \ldots]$

(c) $\sqrt{a^2+1} = [a+1, 2a, 2a, \ldots]$

(d) $\sqrt{a^2-1} = [a-1, \overline{1, 2(a-1)}, \ldots]$

6. Si $\alpha = \frac{P+\sqrt{d}}{Q}$ es un irracional cuadrático con $d \in \mathbb{N}$ libre de cuadrados. ¿Cuál de las siguientes afirmaciones es verdadera?.

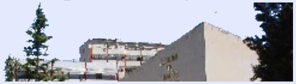
(a) La FCS de α puede ser no periódica.

(b) La FCS de α es puramente periódica.

(c) La FCS de α es periódica con periodo como máximo d.

(d) La FCS de α es periódica con periodo como máximo $2d-1$.

ugr Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra



7. ¿Cuál de las siguientes afirmaciones es verdadera?.

(a) No existen FCS finitas.
(b) Una FCS finita puede ser irracional.
(c) Una FCS finita coincide con su penúltimo convergente.
(d) Una FCS finita coincide con su último convergente.

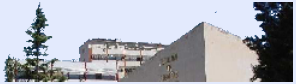
8. Si $\alpha = \frac{P+\sqrt{d}}{Q}$ es un irracional cuadrático, con $d \in \mathbb{N}$ libre de cuadrados. ¿Cuál de las siguientes afirmaciones es verdadera?.

(a) La FCS de α nunca es puramente periódica
(b) La FCS de α siempre es puramente periódica
(c) La FCS de α es puramente periódica si y sólamente si $-1 < \alpha = \frac{a+\sqrt{b}}{c} < 0$ y su conjugado $\overline{\alpha} = \frac{a-\sqrt{b}}{c}$ satisface $1 < \overline{\alpha}$.
(d) La FCS de α es puramente periódica si y sólamente si $1 < \alpha = \frac{a+\sqrt{b}}{c}$ y su conjugado $\overline{\alpha} = \frac{a-\sqrt{b}}{c}$ satisface $-1 < \overline{\alpha} < 0$.

9. Si $\alpha = \sqrt{d}$, con $d \in \mathbb{N}$ libre de cuadrados. ¿La FCS de α es?.

(a) $\alpha = [q_0, \overline{q_1, q_2, \ldots, q_{r-1}, q_r, q_0}]$ con el periodo simétrico.
(b) $\alpha = [q_0, \overline{q_1, q_2, \ldots, q_{r-1}, q_r, q_0}]$ donde cada $q_i < q_0$.
(c) $\alpha = [q_0, \overline{q_1, q_2, \ldots, q_{r-1}, q_r, 2q_0}]$ donde q_0 es el más pequeño.
(d) $\alpha = [q_0, \overline{q_1, q_2, \ldots, q_{r-1}, q_r, 2q_0}]$ donde cada $q_i < q_0$.

ugr Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra



10. Si $x^2 - dy^2 = N$ es una ecuación de Pell, con $|N| < \sqrt{d}$.

(a) Cualquier solución se obtiene de la FCS de $\sqrt{d}$.

(b) Cualquier solución con $\mathrm{mcd}(x, y) = 1$ se obtiene de la FCS de $\sqrt{d}$.

(c) Cualquier solución positiva de la ecuación se obtiene de los convergentes de la FCS de $\sqrt{d}$.

(d) Cualquier solución positiva con $\mathrm{mcd}(x, y) = 1$, son el numerador y denominador de una convergente de la FCS de $\sqrt{d}$.

Final del Test | Puntos:

ugr Universidad de Granada
Enrique R. Aznar
Dpto. de Álgebra