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

CAMPOS CUADRÁTICOS REALES CON NÚMERO DE CLASE PAR

JANETH A. MAGAÑA-ZAPATA MARIO PINEDA-RUELAS

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

1. Introducción

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

El objetivo de este artículo consiste en estudiar la ecuación diofantina

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

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

2. Preliminares

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

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

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

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

3. Fracciones continuas simples

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

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

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

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

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

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

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

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

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

y

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

Entonces

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

Demostración. La prueba es por inducción sobre n y usando

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

□

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

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

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

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

□

Observamos que:

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

En general tenemos:

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

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

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

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

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

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

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

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

Como consecuencia de la afirmación 2 del Teorema 3 tenemos:

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

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

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

Demostración. Ver [7] Teorema 2.1.15. □

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

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

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

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

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

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

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

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

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

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

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

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

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

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

La notación que usaremos es la siguiente:

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

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

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

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

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

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

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

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

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

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

Así que podemos escribir

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

El siguiente resultado es un caso especial del Teorema 14.

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

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

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

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

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

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

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

Por lo anterior

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

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

4. Divisores del número de clase en Campos Cuadráticos Reales

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

4.1. El Orden O_Δ.

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

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

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

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

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

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

donde

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Demostración. El resultado se sigue del Teorema 17. □

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Demostración. Es consecuencia inmediata del Teorema 24. □

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

un O_Δ-ideal primitivo. Entonces

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

Por el Teorema 29 tenemos que

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

Nótese que

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

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

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

Si $n < 0$, siempre se cumple que

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

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

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

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

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

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

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

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

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

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

Si $\sigma = 1$, entonces

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

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

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

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

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

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

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

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

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

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

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

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

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

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

no es de factorización única.

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

Ejemplos de campos cuadráticos con h_Δ par

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

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

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

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

no es de factorización única.

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

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

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

Caso particular de la tabla anterior

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

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

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

Referencias

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

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

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

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