Boletín de Matemáticas
Vol. XVIII Nº 1,2,3 (1984) ***APORTES***

CUERPOS CUADRATICOS EUCLIDIANOS

Iván Castro Chadid

DEFINICION. Sea m un entero distinto de 1 y exento de factores cuadrados.
Diremos que el cuerpo cuadrático $\mathbb{Q}[\sqrt{m}]$ es euclidiano, si el anillo $H[\sqrt{m}]$ de los enteros de $\mathbb{Q}[\sqrt{m}]$ es un anillo euclidiano.

El problema de determinar para qué valores de m, es $\mathbb{Q}[\sqrt{m}]$ euclidiano no ha sido resuelto aún en su totalidad, aunque sí se ha podido determinar en forma precisa cuáles son los enteros m tales que, el valor absoluto de la norma es un algoritmo euclidiano asociado a $H[\sqrt{m}]$.

Esta prueba no es elemental y por el contrario en ella participaron haciendo impor-

tantes aportes durante más de medio siglo muchos matemáticos cuya lista parcial puede encontrarse en el artículo titulado "El algoritmo euclidiano en cuerpo cuadráticos de números", escrito por H. Chatland y publicado en el Bulletin Amer. Math. Soc. 55(1949), (pp.948-953), en donde se dan además las referencias de dichos resultados. Vale la pena recordar que Chatland creyó haber probado que $\mathbb{Q}[\sqrt{97}]$ era euclidiano para el valor absoluto de la norma como algoritmo euclidiano, pero Barbes y Swinnerton-Dyer [Acta Math. 87(1952) 259-323] probaron que $\mathbb{Q}[\sqrt{97}]$ no es euclidiano para esta función.

Para $m < 0$ L.E. Dickson, demostró [L.E. Dickson, Algebren und ihre Zahlentheorie, Zurich and Leipzig 1927, pp.150-151] que el valor absoluto de la norma es un algoritmo euclidiano si y sólo si $m = -1, -2, -3, -7$ y -11.

Finalmente Chatland y Davenport partiendo de todos estos resultados demostraron [Canadian Journal of Math. 2(1950), 289-296] el siguiente teorema:

"El valor absoluto de la norma es un

algoritmo euclidiano asociado a $H[\sqrt{m}]$, si si, $m = -11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17. 19, 21, 29, 33, 37, 41, 57, 73$".

Como puede verse, llegar a este resultado implicó un gran esfuerzo, pero sólo significó una solución particular del mismo.

En el presente artículo pretendemos difundir la prueba de que para $m < 0$, $H[\sqrt{m}]$ es un dominio euclidiano, si si, $m = -11, -7, -3, -2$ y -1 siendo ésta una solución general del problema para valores negativos de m, resultado que como hemos visto va a coincidir con el obtenido para el caso particular del valor absoluto de la norma.

LEMA 1. Si $m = -3, -7$ y -11, $H[\sqrt{m}]$ es un dominio euclidiano.

Demostración. Veamos que el valor absoluto de la norma es un algoritmo euclidiano asociado a $H[\sqrt{m}]$.

Debido a las propiedades de la norma y del valor absoluto, bastaría sólo demostrar que si $\alpha, \beta \in H[\sqrt{m}]$ con $\beta \neq 0$, existen $q, r \in H[\sqrt{m}]$ tales que $\alpha = q\beta + r$ con $|N(r)| < |N(\beta)|$*.

---

* En el presente artículo notaremos la norma de $Z = a + b\sqrt{m}$ como $N(Z) = a^2 - mb^2$.

En efecto

$$\alpha\beta^{-1} = u+v\sqrt{m} \quad \text{en donde } u,v \in \mathbb{Q}.$$

Tomemos $R \in \mathbb{Z}$ tal que $|2v-R| \leq \frac{1}{2}$.

Como $[2u] \leq 2u < [2u] + 1$, tomamos

$$S \in \{[2u],\ [2u] + 1\}.$$

Tal que tenga la misma paridad que R. Luego

$$2|R-S| \quad \text{y} \quad |2u-S| < 1 .$$

Al tener R y S la misma paridad $q = \frac{S+R\sqrt{m}}{2} \in H[\sqrt{m}]$ ya que para estos valores $m \equiv 1 \bmod 4$.

Por otra parte:

$$\begin{aligned}
\alpha - q\beta &= (\alpha\beta^{-1} - q)\beta \\
&= (u+v\sqrt{m} - \frac{S+R\sqrt{m}}{2})\beta \\
&= \frac{\beta}{2}\,((2u-S) + (2v-R)\sqrt{m})
\end{aligned}$$

$$\begin{aligned}
\text{Luego } |N(\alpha-q\beta)| &= \frac{|N(\beta)|}{4}\,|(2u-S)^2 - m(2v-R)^2| \\
&\leq \frac{|N(\beta)|}{4}\,(1 - \frac{m}{4}) \\
&\leq \frac{|N(\beta)|}{4}\,(1 + \frac{11}{4}) \\
&\leq \frac{15}{16}\,|N(\beta)| \\
&< |N(\beta)|
\end{aligned}$$

De donde, si llamamos $r = \alpha - q\beta$ tenemos que

$$\alpha = q\beta + r \text{ con } |N(r)| < |N(\beta)|$$

que es lo que queríamos demostrar.

LEMA 2. Si $m = -1$ y -2, $H[\sqrt{m}]$ es un dominio euclidiano.

Demostración. En una forma similar a la dada en la prueba del Lema 1, vamos a demostrar que si α y $\beta \in H[\sqrt{m}]$ con $\beta \neq 0$, existen $q, r \in H[\sqrt{m}]$ tales que

$$\alpha = \beta q + r \quad \text{con} \quad |N(r)| < |N(\beta)|.$$

En efecto

$$\alpha\beta^{-1} = u + v\sqrt{m} \text{ en donde } u, v \in \mathbb{Q}.$$

Tomemos $x, y \in \mathbb{Z}$ tales que

$$|u - x| \leq \frac{1}{2} \quad \text{y} \quad |v - y| \leq \frac{1}{2}$$

Si $R = u - x$ y $S = v - y$, entonces

$$\alpha\beta^{-1} = (R + X) + (S + Y)\sqrt{m}.$$

Luego

$$\beta(R + S\sqrt{m}) = \alpha - \beta(X + Y\sqrt{m}) \in H[\sqrt{m}].$$

Si $\rho = \beta(R+S\sqrt{m})$, entonces,

$$|N(\rho)| = |N(\beta)|\ |R^2-mS^2|.$$

Pero $|R^2-mS^2| \leq \frac{1}{4} + \frac{2}{4} \leq \frac{3}{4}$.

De donde $|N(\rho)| \leq |N(\beta)|\ \frac{3}{4} < |N(\beta)|$ lo cual completa la demostración.

OBSERVACION 1. Recordemos que si $\mathcal{D}$ es un dominio entero con unidad y S un subconjunto de $\mathcal{D}$, el conjunto derivado S' de S, se define como $S' = S \cap B$ en donde

$$B = \{b \in \mathcal{D} \ / \ \exists\, a \in \mathcal{D} \text{ y } a+b\mathcal{D} \subseteq S\}.$$

Además si $\mathcal{D}_o = \mathcal{D}-\{0\}$ entonces $\mathcal{D}_n = \mathcal{D}'_{n-1}\ \forall n \geq 1$.

Se sabe (ver [5] observación 3) que una condición necesaria y suficiente para la existencia de algún algoritmo euclidiano asociado a $\mathcal{D}$ es que la $\bigcap_{n=0}^{\infty} \mathcal{D}_n = \emptyset$.

Vamos a apoyarnos en este hecho para poder cumplir con el objetivo que nos hemos propuesto.

Veamos el siguiente lema en donde se da una definición alternativa de conjunto derivado.

LEMA 3. $S' = \{b \in S \;/\; \exists\, a \in \mathcal{D},\ \forall c \in \mathcal{D} - S,\ a+c \notin \langle b\rangle\}$

Demostración. Sea

$$T = \{b \in S \;/\; \exists\, a \in \mathcal{D},\ \forall c \in \mathcal{D}-S,\ a+c \notin \langle b\rangle\}$$

1) Si $b \in T$, entonces, $b \in S$ y existe $a \in \mathcal{D}$ tal que $\forall c \in \mathcal{D}-S$, $a+c \notin \langle b\rangle$. Por lo tanto, $\forall c \in \mathcal{D}-S$ y $\forall \alpha \in \mathcal{D}$, $c \neq -a+\alpha b$. De donde $\forall \alpha \in \mathcal{D}$, $-a+\alpha b \notin \mathcal{D}-S$, luego $-a+\alpha b \in S$, $\forall \alpha \in \mathcal{D}$. De lo anterior se desprende que $-a+b\mathcal{D} \subseteq S$ y por consiguiente $b \in S \cap B = S'$.

2) Sea $b \in S \cap B$, entonces, $b \in S$ y existe $a \in \mathcal{D}$ tal que $a+b\mathcal{D} \subseteq S$. Si existiera $c \in \mathcal{D}-S$ tal que $-a+c \in \langle b\rangle$, entonces, $c = a+\alpha b$ para algún $\alpha \in \mathcal{D}$. Pero $a+\alpha b \in a+b\mathcal{D} \subseteq S$, entonces, $c \in S$. Lo cual es una contradicción.

Luego $\forall c \in \mathcal{D}-S$, $-a+c \notin \langle b\rangle$. Por lo tanto $b \in T$.

EJERCICIO.

Si $\mathcal{D}_0 = \mathcal{D}-\{0\}$, entonces $\mathcal{D}_1 = \mathcal{D}_0' = \mathcal{D}-(\mathcal{D}^* \cup \{0\})$ en donde $\mathcal{D}^*$ es el conjunto de unidades de $\mathcal{D}$.

Desarrollo. Sea $b \in \mathcal{D}_1$, entonces, existe $a \in \mathcal{D}$ tal que $a \notin \langle b \rangle$. Luego $b \notin \mathcal{D}^*$ y como $b \neq 0$, entonces $b \in \mathcal{D}-(\mathcal{D}^* \cup \{0\})$.

Por otra parte, si $d \in \mathcal{D}-(\mathcal{D}^* \cup \{0\})$, entonces $d \notin \mathcal{D}^* \cup \{0\}$. Por lo tanto d no divide a 1. De donde $1 \notin \langle d \rangle$ y por lo tanto $d \in \mathcal{D}_1$.

DEFINICIONES.

1) Sea $b \in \mathcal{D}-(\mathcal{D}^* \cup \{0\})$, b se denomina un *divisor de lado* de $a \in \mathcal{D}$, si existe $e \in \mathcal{D}^* \cup \{0\}$ tal que $b \mid a + e$.

2) Sea $b \in \mathcal{D}-(\mathcal{D}^* \cup \{0\})$, b se denomina un *divisor universal de lado de* $\mathcal{D}$, si b es un divisor de lado de a, $\forall a \in \mathcal{D}$.

OBSERVACION 2.

$\mathcal{D}_2 = \{b \in \mathcal{D}-(\mathcal{D}^* \cup \{0\}) / \ b$ no es divisor universal de lado de $\mathcal{D}\}$

LEMA 4. Si $\mathcal{D}$ no es un cuerpo y no tiene divisores universales de lado, entonces, no es euclidiano.

Demostración. Si $\mathcal{D}$ no tiene divisores universales de lado, entonces $\mathcal{D}_2 = \mathcal{D}-(\mathcal{D}^* \cup \{0\}) = \mathcal{D}_1$ de donde $\mathcal{D}_n = \mathcal{D}_1$, $\forall n \in \mathbb{N}$.

Luego $\bigcap_{n=0}^{\infty} \mathcal{D}_n = \mathcal{D}_1 \neq \emptyset$. (Si $\mathcal{D}$ fuese un cuerpo $\mathcal{D}_1 = \emptyset$) de donde se tiene que $\mathcal{D}$ no es euclidiano.

LEMA 5. ± 2 y ± 3 son irreducibles en $H[\sqrt{-m}]$, $(m > 0)$, si si, $m \neq 1,2,3,7$ y 11.

Demostración. $\Rightarrow$) Si ± 2 y ± 3 son irreducibles en $H[\sqrt{-m}]$ entonces:

a) $m \neq 1$ ya que $2 = (1+i)(1-i)$ y ninguno de estos valores es una unidad de $H[\sqrt{-1}]$.

b) $m \neq 2$ por que $3 = (1+\sqrt{2}i)(1-\sqrt{2}i)$ y ninguno de estos factores es una unidad de $H[\sqrt{-2}]$.

c) $m \neq 3$ debido a que $3 = (0+\sqrt{3}i)(0-\sqrt{3}i)$ y estos dos elementos no son unidades de $H[\sqrt{-3}]$.

d) $m \neq 7$, ya que $2 = (1/2+(1/2)\sqrt{-7})(1/2-(1/2\sqrt{-7})$ y estos factores no son unidades de $H[\sqrt{-7}]$.

e) $m \neq 11$, por que $3 = (1/2+(\sqrt{11}/2)i)(1/2 - (\sqrt{11}/2)i)$ y estos factores no son unidades de $H[\sqrt{-11}]$.

$\Leftarrow$) **1)** Supongamos que 2 es reducible en $H[\sqrt{-m}]$ para algún $m \neq 1,2,3,7,11$ entonces -2 también lo es.

Luego existen Z, $W \in H[\sqrt{-m}]$ ninguna de las dos unidades, tales que $2 = ZW$. Entonces $N(2) = N(Z)N(W)$. De donde $4 = N(Z)N(W)$. Como $N(Z) \neq 1$ y $N(W) \neq 1$ por no ser unidades entonces $N(Z) = 2$. Se presentan las siguientes posibilidades.

1. Que $Z = a+bi\sqrt{m}$ con $a,b \in \mathbb{Z}$.
En este caso la ecuación $N(Z) = 2$ se transforma en $a^2+b^2 m = 2$.

.) Si $b = 0$, entonces $a^2 = 2$ lo cual implica que $x^2 - 2$ es reducible sobre $\mathbb{Q}$ pero este hecho contradice el criterio de Eisenstein para $p = 2$.

.) Si $b \neq 0$, entonces $b^2 m \geq 5$ y por lo tanto $a^2+b^2 m > 2$ lo cual también es una contradicción.

2. Que $Z = (a+1/2)+(b+1/2)\sqrt{m}i$, con $a,b \in \mathbb{Z}$.

En este caso la ecuación $N(Z) = 2$ se transforma en $(a+1/2)^2+(b+1/2)^2 m = 2$ y además $-m \equiv 1 \mod 4$ (ver [1] Teorema 238), como en particular $m \neq 3$, 7 y 11, entonces $m > 11$. Luego $(b+1/2)^2 m \geq (b+1/2)^2 11 \geq \frac{11}{4} > 2$. Lo cual nos conduce a una contradicción.

2) Supongamos que 3 es reducible en $H[\sqrt{-m}]$ para algún $m \neq 1,2,3,7$ y 11 entonces -3 también lo es.

Luego existen $Z, W \in H[\sqrt{-m}]$ ninguna de las dos unidades, tales que $3 = ZW$.

Entonces $N(3) = N(Z)N(W)$. De donde $9 = N(Z)N(W)$.

Como $N(Z) \neq 1$ y $N(W) \neq 1$, entonces $N(Z) = 3$. Se presentan las siguientes posibilidades.

1. Que $Z = a+bi\sqrt{m}$, con $a, b \in \mathbb{Z}$.
En este caso la ecuación $N(Z) = 3$ se transforma en $a^2+b^2m = 3$.

.) Si $b = 0$, entonces $a^2 = 3$ lo cual implica que x^2-3 es reducible sobre $\mathbb{Q}$ pero este hecho contradice el criterio de Eisenstein para $p = 3$.

.) Si $b \neq 0$, entonces $b^2m \geq 5$ y por lo tanto $a^2+b^2m > 3$, lo cual también es una contradicción.

2. Que $Z = (a+1/2)+(b+1/2)i\sqrt{m}$, con $a, b \in \mathbb{Z}$.
En este caso la ecuación $N(Z) = 3$ se transforma en

$$(a+1/2)^2 + (b+1/2)^2m = 3$$

y además $-m \equiv 1 \bmod 4$. Como $m \neq 3$, 7 y 11, entonces $m \geq 15$. Luego $(b+1/2)^2 m \geq (b+1/2)^2 15 \geq \frac{15}{4} > 3$, lo cual nos conduce a una contradicción.

LEMA 6. Los únicos divisores de lado de 2 en $H[\sqrt{-m}]$ $(m > 0)$, $m \neq 1,2,3,7$ y 11 son ± 2 y ± 3.

Demostracion. $\pm 2 \mid 2 + 0$ y $\pm 3 \mid 2 + 1$. Además si $b \in H[\sqrt{-m}] - \{0, \pm 1\}$ es tal que $b \mid 2 + e$ para algún $e \in \{0,1,-1\}$ y $b \neq \pm 2, \pm 3$, entonces existe $\alpha \in H[\sqrt{-m}]$ tal que $\alpha b = 2 + e$. Se presentan las siguientes posibilidades:

1) Que $e = 0$. Entonces $\alpha b = 2$ y por lo tanto 2 es reducible en $H[\sqrt{-m}]$ lo cual contradice el Lema 5.

2) Que $e = 1$. Entonces $\alpha b = 3$ y por lo tanto 3 es reducible en $H[\sqrt{-m}]$ lo cual también contradice el Lema 5.

3) Que $e = -1$. Entonces $\alpha b = 1$, luego b es una unidad de $H[\sqrt{-m}]$ pero para $m > 0$, $m \neq 1,3$, las unidades de $H[\sqrt{-m}]$ son 1 y -1 (ver [1] Teorema 9.22) lo cual también es una contradicción.

LEMA 7. Si $-m \not\equiv 1 \bmod 4$, entonces ± 2 no es un divisor de lado de $i\sqrt{m}$.

Demostración. Es suficiente el demostrar que 2 no es un divisor de lado de $i\sqrt{m}$. Supongamos que 2 es divisor de lado de $i\sqrt{m}$, entonces existe $e \in \{0, \pm 1\}$, tal que $2 \mid i\sqrt{m} + e$.

Luego existe $\alpha \in H[\sqrt{-m}]$ tal que $2 = e+i\sqrt{m}$. $\alpha = a+bi\sqrt{m}$ con $a,b \in \mathbb{Z}$, entonces $2a = e$ y $2b = 1$ lo cual es absurdo.

LEMA 8. Si $-m \not\equiv 1 \bmod 4$, entonces ± 3 no es divisor de lado de $i\sqrt{m}$.

Demostración. Si $3 \mid i\sqrt{m}+e$ para algún $e \in \{0,1,-1\}$, existe $\alpha \in H[\sqrt{-m}]$ tal que $3\alpha = i\sqrt{m}+e$. $\alpha = a+bi\sqrt{m}$ con $a,b \in \mathbb{Z}$, entonces $3a = e$ y $3b = 1$ lo cual es absurdo.

LEMA 9. Si $-m \equiv 1 \bmod 4$, entonces ± 2 no es divisor de lado de $1/2 + i/2\sqrt{m}$.

Demostración. Si $2 \mid 1/2 + i/2\sqrt{m} + e$ para algún $e \in \{0,1,-1\}$, existe $\alpha \in H[\sqrt{-m}]$ tal que $2\alpha = 1/2 + e + i/2\sqrt{m}$.

α debe ser de la forma $(a+1/2)+(b+1/2)i\sqrt{m}$ para algunos $a,b \in \mathbb{Z}$. Luego $2a+1 = 1/2 + e$ y $2b + 1 = 1/2$, lo cual es absurdo.

LEMA 10. Si $-m \equiv 1 \bmod 4$, entonces ± 3 no es divisor de lado de $1/2 + i/2\sqrt{m}$.

Demostración. Supongamos que $3 \mid 1/2 + i/2\sqrt{m}+e$ para algún $e \in \{0,1,-1\}$, existe $\alpha \in H[\sqrt{-m}]$ tal que $3\alpha = 1/2 + e + i/2\sqrt{m}$.

α debe ser de la forma $(a+1/2)+(b+1/2)i\sqrt{m}$ para algunos, $a,b \in \mathbb{Z}$. Luego $3a+3/2 = 1/2 + e$ y $3b+3/2 = 1/2$ lo cual es absurdo.

LEMA 11. Si $m > 0$, $m \neq 1,2,3,7,11$, $H[\sqrt{-m}]$ no tiene divisores universales de lado.

Demostración. Si α fuese un divisor universal de lado de $H[\sqrt{-m}]$, entonces α sería en particular divisor de lado de 2.

Pero los únicos divisores de lado de 2 en $H[\sqrt{-m}]$ son ± 2 y ± 3 (Lema 6). De los Lemas 7, 8, 9 y 10 se desprende que ± 2 y ± 3 no son divisores universales de lado de $H[\sqrt{-m}]$, $m \neq 1,2,3,7$ y 11. Luego $H[\sqrt{-m}]$ no tiene divisores universales de lado para estos valores de m.

LEMA 12. Si $m > 0$, $m \neq 1,2,3,7$ y 11, $H[\sqrt{-m}]$ no es un dominio euclidiano.

Demostración. $H[\sqrt{-m}]$ no es un cuerpo y tampoco tiene divisores universales de lado (Lema 11) por lo tanto no es un dominio euclidiano (Lema 4).

TEOREMA. $H[\sqrt{m}]$ para $m < 0$ es un dominio euclidiano, si si, $m = -1, -2, -3, -7$ y -11.

Demostración. Consecuencia inmediata de los lemas **1, 2 y 12.**

BIBLIOGRAFIA

[1] Hardy and Wright, *An Introduction to the theory of numbers*, Fifth Edition. Oxford at the Carendon Press, 1979 (Capítulo XIV).

[2] H. Chatland, "On the euclidean algorithm in quadratic number fields", Bull. Amer. Math. Soc. Vol.55 (1949) pp.948-953.

[3] Niven y Zuckerman, *Introducción a la Teoría de los Números*, Limusa Wiley, S.A. México 1969. (Capítulo IX).

[4] C. Mutaflan, *Algebra II: Anillos, campos y teoría de Galois*, C.E.C.S.A. México, 1976, pp. 298 a 300.

[5] I. Castro, "Una forma conjuntista de enfocar los dominios euclidianos", Matemática, enseñanza universitaria, Nº 31 Junio 1984, pp. 3-14.

[6] T.H. Motzkin, "The euclidean algorithm", Bull. Amer. Math. Soc. Vol.55 (1949) pp. 1142-1146.

* *

Departamento de Matemáticas y Estadística.
Universidad Nacional
BOGOTA. D.E. Colombia.