Pub. Mat. UAB
Vol. 26 Nº 2 Juny 1982

CUERPOS CUBICOS Y CUERPO DE CLASES DE CUERPOS CUADRATICOS REALES*

Pascual Llorente

Rebut el 2 de febrer del 1982

1. INTRODUCCION

Sea K un cuerpo cuadrático (extensión cuadrática del cuerpo Q de los números racionales) de discriminante D. Es sabido que $D \equiv 0, 1 \pmod 4$ es un entero que determina unívocamente a K. Sean $G(D)$ el grupo de clases de ideales de K y $h(D)$ el orden de $G(D)$.

Recordemos que si G es un grupo abeliano y q un primo, el q-rango de G es el número de factores cíclicos de la componente q-primaria de G (o, equivalentemente, la dimensión del Z_q-espacio vectorial G/qG). Denotaremos con $r_q(D)$ al q-rango del grupo abeliano $G(D)$.

El estudio de $r_2(D)$ quedó prácticamente completado por Gauss con su teoría de los géneros. En efecto, $r_2(D)$ es una función creciente del número de primos distintos que dividen a D. Muy poco se conoce aún sobre $r_q(D)$ si $q > 2$.

En los últimos años se han encontrado muchos ejemplos de D con $r_3(D) > 1$ en el caso $D < 0$ (K imaginario) pero se conocen pocos ejemplos de $D > 0$ (K real) con $r_3(D) > 1$. Particularmente interesante es el caso en que $D = p > 0$ es primo. De la observación de las tablas existentes se conjeturaba que $r_q(p) \leq 2$ para $q > 2$, hasta que en [9] se mostró que si $p = 188184253$ (primo) entonces $r_3(p) = 3$; en efecto, $G(188184253) \simeq Z_3 \oplus Z_3 \oplus Z_3$.

La determinación de $h(D)$ y de $G(D)$ se puede efectuar en un número finito de pasos pero los algoritmos clásicos resultan irrealizables cuando $|D|$ es relativamente grande, aún utilizando un computador veloz. E. Lehmer y D. Shanks (ver [8]) han hallado un método para calcular $h(D)$ y determinar $G(D)$ que funciona particular-

*Este trabajo fué presentado en el II Congreso Venezolano de Matemáticas (Cumaná, 28/31 de marzo de 1979).

mente bien en el caso $D < 0$. La dificultad en el caso $D > 0$ se debe a la necesidad de conocer un inversible fundamental de K. Utilizando dicho método Buell |1| construyó una tabla de $h(D)$ y $G(D)$ para $0 > D > -4 \cdot 10^6$. Actualmente se conocen varios $D < 0$ tales que $r_3(D) = 3$ pero para $D > 0$ el ejemplo dado anteriormente es el único conocido. De la tabla de Buell y de una conocida relación que existe entre $r_3(-3D)$ y $r_3(D)$ se deduce que si p es un primo tal que $r_3(p) > 2$ entonces $p > 1.333.333$.

Sea $H(D)$ el cuerpo de clases de Hilbert de K, es decir, la máxima extensión abeliana no ramificada de K. Es sabido que $Gal\ (H(D) / K) \simeq G(D)$. Sea $H_3(D)$ la composición de todas las extensiones cúbicas cíclicas no ramificadas de K. Entonces $H_3(D)$ es el subcuerpo de $H(D)$ tal que

$$Gal\ (H_3(D) / K) \simeq Z_3^{\,r_3(D)}$$

Es claro que $H(D)$ contiene toda la información sobre $G(D)$ y que el conocimiento de $H_3(D)$ implica, en particular, el de $r_3(D)$, pero sobre la determinación efectiva de estos cuerpos por métodos aritmético-algebraicos sólo se conocen resultados parciales (ver |5|).

En este trabajo el autor se propone hallar un método para determinar $H_3(D)$ y, en consecuencia, $r_3(D)$. Aunque el método puede ser generalizado a los casos en que $D \not\equiv 0 \pmod 3$ es libre de cuadrados (y aún para $D < 0$), por lo visto anteriormente se considera sólo el caso en que $D = p > 0$ es primo.

El primer resultado obtenido traslada el problema (y lo vincula) a otro problema abierto en la Teoría de Números Algebraicos.

En efecto, utilizando resultados conocidos de la Teoría de Cuerpos de Clases (ver |5|) se prueba el siguiente

TEOREMA 1.1 *Sea K un cuerpo cuadrático de discriminante $D > 0$ libre de cuadrados. Las extensiones cúbicas cíclicas no ramificadas de K están en correspondencia biyectiva con las ternas de cuerpos cúbicos conjugados de discriminante D.*

COROLARIO 1.2 *Sea K un cuerpo cuadrático de discriminante $D > 0$ libre de cuadrados. Para determinar $H_3(D)$ y $r_3(D)$ es suficiente determinar todas las ternas (E_i, E_i', E_i'') con $i = 1, 2, \ldots, r$ de cuerpos cúbicos conjugados de discriminan-*

te D. En efecto, en tal caso $H_3(D) = K \cdot E_1 \dots E_n$ *y* $r_3(D) = \log_3 (2n+1)$.

Los cuerpos cúbicos E de discriminante $D > 0$ libre de cuadrados son cuerpos cúbicos reales no cíclicos (es decir, E y sus conjugados son reales y distintos). De los resultados anteriores se deduce que $r_3(D) > 1$ (con $D > 0$ libre de cuadrados y $D \equiv 1 \pmod 4$) si y sólo si existen al menos dos cuerpos cúbicos no conjugados de discriminante D. En tal caso existen al menos cuatro de tales cuerpos (pues $r_3(D) \geq 2$) y existen al menos trece si $r_3(D) > 2$.

Godwin y Samet en [4] construyen una tabla de los cuerpos cúbicos reales de discriminante D para $0 < D < 20000$ y observan que no existen cuerpos cúbicos no cíclicos no conjugados con el mismo discriminante D si $D < 20000$, pero señalan que Heilbroun ha descubierto que existen dos cuerpos cúbicos no conjugados de discriminante $D = 130397 = 19 \cdot 6863$.

Sea desde ahora D un entero positivo libre de cuadrados y congruente con 1 módulo 4. Como nos interesaremos particularmente en el caso en que $D = p$ es primo, supondremos también que $D \not\equiv 0 \pmod 3$. Siendo $h(5) = 1$ supondremos finalmente que $D > 5$.

Cada terna de cuerpos cúbicos conjugados de discriminante D queda determinada por un polinomio irreducible

$$f(a,b,x) = x^3 - ax + b$$

donde a y b son enteros positivos tales que

i) No existe ningún entero $n > 1$ tal que $n^2 \mid a$ y $n^3 \mid b$.

ii) El discriminante $D(a,b)$ de $f(a,b,x)$ verifica

$$D(a,b) = 4a^3 - 27b^2 = D\delta^2$$

para algún entero $\delta \geq 1$.

iii) Si $a \not\equiv 0 \pmod 3$ entonces existen enteros k y h tales que

$$3t^2 - a = k\delta$$

y

$$t^3 - at + b = h\delta^2$$

para algún entero t tal que $-\delta/2 < t \leq \delta/2$.
En tal caso, si α es una raíz de $f(a,b,x)$ entonces $1, \alpha, \frac{\alpha^2 - t\alpha + (t^2-a)}{\delta}$
es una base de los enteros del cuerpo cúbico $E = Q(\alpha)$.

iv) Si $a = 3a_1 \equiv 0 \pmod 3$ entonces $a \equiv 3 \pmod 9$ (es decir $a_1 = 3a_2 + 1$ para algún entero a_2), $b \equiv \pm (a-1) \pmod{27}$, $\delta = 27\,\delta_0$ para algún entero $\delta_0 \geq 1$ y existen enteros k y h tales que

$$3t^2 - a = 9\,\delta_0\,k$$

y

$$t^3 - at + b = 27\,\delta_0^2\,h$$

para algún entero t tal que $-3\,\delta_0/2 < t \leq 3\,\delta_0/2$.
En tal caso, si α es una raíz de $f(a,b,x)$ entonces

$$1, \quad \frac{\alpha - t}{3}, \quad \frac{\alpha^2 + t\alpha + (t^2 - a)}{9\,\delta_0}$$

es una base de los enteros del cuerpo cúbico $E = Q(\alpha)$.

Los resultados anteriores constituyen el conocido Teorema de Voronoi (ver |2|, pag. 112) aplicado a nuestro caso y las notaciones introducidas quedan fijadas para el resto de este trabajo.

Un método para determinar todos los cuerpos cúbicos de discriminante D consiste en

a) Resolver la ecuación diofántica

$$4a^3 - 27b^2 = D\,\delta^2$$

con las condiciones impuestas por el Teorema de Voronoi.

b) Determinar cuándo dos soluciones (a_1, b_1, δ_1) y (a_2, b_2, δ_2) definen cuerpos conjugados.

Además, para que el método sea efectivamente computable, es necesario establecer cotas para las soluciones. En este trabajo se observa que este problema puede resolverse junto con el b) con métodos diferentes a los utilizados en |2| y en |4|. Para ello asociamos a cada solución de a) una forma cuadrática $F(a,b)$ de discriminante $-3D$ de la siguiente manera:

DEFINICION 1.3 i) Si $a \not\equiv 0 \pmod 3$ entonces $F(a,b) = (A, B, C)$ donde

$$A = 3k^2 - 27th$$

$$B = 3kt - 9hs$$

$$C = a$$

ii) Si $a \equiv 0 \pmod 3$, sean $k = 3k_0 + \varepsilon$ y $t = 3t_0 + \delta$ con $|\varepsilon| \leq 1$ y $|\delta| \leq 1$ y sea $\mu = \varepsilon\delta$. Entonces $F(a,b) = (A, B, C)$ donde

$$A = kk_0 + 2\varepsilon k_0 - ht + \mu kt_0 - 3\mu hs_0 + \mu^2 a_2 + \mu^2$$

$$B = kt + 2\mu a_1 - 9sh$$

$$C = a$$

La forma cuadrática $F(a,b)$ representa los coeficientes del término de primer grado del polinomio minimal de los enteros del cuerpo de traza nula. Entonces, utilizando resultados de la teoría de formas cuadráticas (ver |3|) se prueba

TEOREMA 1.4 *i) Dos soluciones de a) definen cuerpos cúbicos conjugados si y sólo si las formas cuadráticas asociadas son iguales u opuestas.*

ii) Toda terna de cuerpos cúbicos conjugados de discriminante D está definida por una solución de a) con $a < \sqrt{D}$.

La cota $a < \sqrt{D}$ implica $s < 2\sqrt[4]{D}$ (luego $s_0 < \frac{2\sqrt[4]{D}}{27}$ si $a \equiv 0 \pmod 3$), pero estos resultados resultan insuficientes para estudiar los casos en que D es relativamente grande. La computabilidad efectiva depende del estudio congruencial de la ecuación diofántica $4a^3 - 27b^2 = D s^2$ respecto de distintos módulos. Particularmente importante es el estudio congruencial módulo 27 de dicha ecuación en el caso $a \not\equiv 0 \pmod 3$. Los resultados de dicho estudio están contenidos en la Tabla 1.

TABLA 1

Estudio de $4a^3 - 27b^2 = Dd^2 \pmod{27}$

D (mod 27)	a (mod 9)	d (mod 27)
1	1	2 , 25
	4	11 , 16
	7	7 , 20
4	1	1 , 26
	4	8 , 19
	7	10 , 17
7	1	4 , 23
	4	5 , 22
	7	13 , 14
10	1	7 , 20
	4	2 , 25
	7	11 , 16
13	1	10 , 17
	4	1 , 26
	7	8 , 19
16	1	13 , 14
	4	4 , 23
	7	5 , 22
19	1	11 , 16
	4	7 , 20
	7	2 , 25
22	1	8 , 19
	4	10 , 17
	7	1 , 26
25	1	5 , 22
	4	13 , 14
	7	4 , 23

D (mod 27)	a (mod 9)	d (mod 27)
2	2	4 , 23
	5	13 , 14
	8	5 , 22
5	2	1 , 26
	5	10 , 17
	8	8 , 19
8	2	2 , 25
	5	7 , 20
	8	11 , 16
11	2	5 , 22
	5	4 , 23
	8	13 , 14
14	2	8 , 19
	5	1 , 26
	8	10 , 17
17	2	11 , 16
	5	2 , 25
	8	7 , 20
20	2	13 , 14
	5	5 , 22
	8	4 , 23
23	2	10 , 17
	5	8 , 19
	8	1 , 26
26	2	7 , 20
	5	11 , 16
	8	2 , 25

Una vez concluída la elaboración teórica del método, se lo expresó en lenguaje FORTRAN IV y se obtuvo el programa RANG3 que calcula todos los cuerpos cúbicos de discriminante D dado y, por lo tanto, $H_3(D)$ y $r_3(D)$. Cada terna de cuerpos cúbicos conjugados está dada por el par de enteros $(a;b)$ (es decir, por el polinomio $f(a,b,x)$) con a mínimo. El programa también calcula δ y t y da, por lo tanto, una base de los enteros de cada cuerpo. Por último el programa calcula la forma cuadrática asociada en su forma reducida, lo que permite determinar inmediatamente si dos pares $(a_1 ; b_1)$ y $(a_2 ; b_2)$ corresponden o no a la misma terna de cuerpos cúbicos.

RANG3 recorre todos los valores posibles de $a \not\equiv 0 \pmod 3$ y δ dentro de las cotas establecidas y de acuerdo con las condiciones de la Tabla 1. En el caso $a = 3a_1$ recorre todos los valores de $a_1 \equiv 1 \pmod 3$ y δ_0 dentro de las cotas establecidas. Para aquellos pares $(a;\delta)$ tales que $(4a^3 - D\delta^2)/27$ (respectivamente $4a_1^3 - 27D\delta_0^2$ si $a = 3a_1$) es el cuadrado de un entero $b > 0$, verifica la existencia de los enteros t, k y h, y los calcula, mediante la subrutina TKH (respectivamente: TKH3 si $a = 3a_1$). Entonces calcula $F(a;b)$ usando la Definición 1.3 y la lleva a su forma reducida mediante la subrutina REDUC.

RANG3 también se adaptó al lenguaje de una computadora HP-97.

Con estos elementos se hicieron varias computaciones. En particular se construyó una tabla de todos los cuerpos cúbicos de discriminante $D = p$ primo para $1 < p < 10^6$ y se obtuvieron varios primos p con $r_3(p) > 1$ en el sector $1333333 < p < 9 . 10^6$ (para todos ellos es $r_3(p) = 2$).

En las dos próximas secciones se dan algunos resultados obtenidos en relación con cada uno de los problemas planteados.

2. SOBRE CUERPOS CUBICOS REALES NO CICLICOS CON EL MISMO DISCRIMINANTE

Observando la tabla de todos los cuerpos cúbicos de discriminante $D = p$ primo para $1 < p < 10^6$ podemos asegurar

TEOREMA 2.2 *Existen 30 primos $p \equiv 1 \pmod 4$, $1 < p < 10^6$ con más de un cuerpo cúbico de discriminante $D = p$, el menor de los cuales es $p = 32009$. Para*

TABLA 2

Primos $D \equiv 1 \pmod 4$, $1 < D < 10^6$ con más de un cuerpo cúbico de discriminante D

D		a	b	Δ	t
32009	E_1:	41	95	1	
	E_2:	59	171	1	
	E_3:	83	94	8	3
	E_4:	143	301	17	5
62501	E_1:	26	17	1	
	E_2:	188	991	1	
	E_3:	206	1137	1	
	E_4:	131	430	8	3
114889	E_1:	37	57	1	
	E_2:	127	547	1	
	E_3:	181	935	1	
	E_4:	211	1058	8	-3
142097	E_1:	35	33	1	
	E_2:	125	533	1	
	E_3:	203	950	8	-1
	E_4:	245	811	17	5
151141	E_1:	34	15	1	
	E_2:	178	911	1	
	E_3:	307	1982	8	3
	E_4:	364	2351	17	-5
153949	E_1:	34	11	1	
	E_2:	52	123	1	
	E_3:	163	526	8	3
	E_4:	157	56	10	-3
220217	E_1:	47	85	1	
	E_2:	371	2749	1	
	E_3:	395	2934	8	-1
	E_4:	345	371	1(27)	1

D		a	b	Δ	t
255973	E_1:	40	1	1	
	E_2:	94	337	1	
	E_3:	274	1743	1	
	E_4:	316	1391	17	-3
275881	E_1:	61	153	1	
	E_2:	151	707	1	
	E_3:	313	2129	1	
	E_4:	193	208	10	-1
282461	E_1:	194	1035	1	
	E_2:	299	1814	8	-1
	E_3:	533	544	46	-3
	E_4:	372	7	1(27)	-1
321053	E_1:	44	27	1	
	E_2:	134	587	1	
	E_3:	368	2715	1	
	E_4:	347	2330	8	1
363397	E_1:	46	31	1	
	E_2:	100	367	1	
	E_3:	316	2159	1	
	E_4:	313	1788	10	-1
412277	E_1:	50	57	1	
	E_2:	86	281	1	
	E_3:	410	3193	1	
	E_4:	443	3450	8	1
422573	E_1:	404	3123	1	
	E_2:	275	1441	8	-3
	E_3:	317	1776	10	-3
	E_4:	426	209	1(27)	1

D		a	b	δ	t
449797	E_1:	82	255	1	
	E_2:	430	2639	17	8
	E_3:	444	907	1(27)	-1
	E_4:	480	2059	1(27)	-1
486221	E_1:	74	205	1	
	E_2:	128	541	1	
	E_3:	462	1217	1(27)	1
	E_4:	534	3071	1(27)	1
529393	E_1:	55	71	1	
	E_2:	73	195	1	
	E_3:	355	2318	8	3
	E_4:	607	3019	35	-12
578581	E_1:	208	893	5	-1
	E_2:	262	1459	5	-2
	E_3:	442	3501	5	2
	E_4:	643	2258	40	-11
602521	E_1:	319	2110	4	1
	E_2:	187	641	5	2
	E_3:	367	2601	5	2
	E_4:	403	3023	5	-1
621749	E_1:	158	93	5	-1
	E_2:	308	661	13	4
	E_3:	581	4232	22	5
	E_4:	752	2777	49	13
635909	E_1:	74	191	1	
	E_2:	92	303	1	
	E_3:	611	5682	8	-3
	E_4:	692	4499	35	3
686977	E_1:	175	622	4	1
	E_2:	553	3405	23	-10
	E_3:	571	1769	31	5
	E_4:	615	3989	1(27)	1

D		a	b	δ	t
729293	E_1:	80	221	1	
	E_2:	674	6733	1	
	E_3:	608	457	35	11
	E_4:	570	2783	1(27)	1
775661	E_1:	128	531	1	
	E_2:	251	710	8	-1
	E_3:	734	7091	17	1
	E_4:	642	4273	1(27)	-1
783689	E_1:	149	679	1	
	E_2:	167	813	1	
	E_3:	689	6959	1	
	E_4:	299	1450	8	1
785269	E_1:	289	1860	2	1
	E_2:	544	4509	11	3
	E_3:	427	2022	16	3
	E_4:	661	888	38	9
829813	E_1:	88	265	1	
	E_2:	160	759	1	
	E_3:	570	2243	1(27)	1
	E_4:	660	4493	1(27)	1
893029	E_1:	226	1295	1	
	E_2:	283	1114	8	1
	E_3:	856	117	53	12
	E_4:	696	5083	1(27)	-1
902333	E_1:	212	759	5	-2
	E_2:	425	2196	14	5
	E_3:	552	745	1(27)	-1
	E_4:	570	1753	1(27)	-1
946733	E_1:	128	525	1	
	E_2:	614	5853	1	
	E_3:	920	10739	1	
	E_4:	251	314	8	1

cada uno de ellos existen exactamente 4 ternas de cuerpos cúbicos conjugados.

En la Tabla 2 se dan los 30 primos del Teorema 2.2 y, para cada uno de ellos los cuatro polinomios irreducibles $f(a,b,x) = x^3 - a\,x + b$ que definen los cuerpos cúbicos correspondientes y los valores de δ y t que permiten determinar una base de los enteros de cada uno de dichos cuerpos cúbicos.

En la Tabla 2 se encuentran tres valores de D menores que 130397 (dado en |4|). También se ha determinado que existen cuatro ternas de cuerpos cúbicos conjugados de discriminante $D = 42817 = 47 \cdot 911$.

Los 104 primos de la Tabla 8 son otros ejemplos de primos $p \equiv 1 \pmod 4$ con más de un cuerpo cúbico de discriminante $D = p$.

En la Tabla 3 se dan las 13 ternas de cuerpos cúbicos conjugados de discriminante $D = 188184253$. Para cada una de ellas se dan, además de los valores de a, b, δ y t, la forma cuadrática asociada $F(a,b) = (A,B,C) = A\,x^2 + B\,x\,y + C\,y^2$.

TABLA 3

Cuerpos cúbicos de discriminante $D = 188184253$

E	a	b	δ	t	$F(a,b)$
E_1	370	731	1		(370 , -81 , 381459)
E_2	604	5067	1		(604 , -301 , 233710)
E_3	694	6523	1		(694 , 411 , 203430)
E_4	2260	41269	1		(2260 , 781 , 62518)
E_5	2011	27546	8	1	(2011 , -1327 , 70402)
E_6	3235	67598	8	3	(3235 , -2401 , 44074)
E_7	7807	28206	100	37	(7807 , 821 , 18100)
E_8	9952	192671	125	22	(9952 , 3363 , 14466)
E_9	10156	112539	143	142	(10156 , 7509 , 15285)
E_{10}	6330	180263	1 (27)	1	(6330 , -399 , 22303)
E_{11}	9462	347015	1 (27)	1	(9462 , -6333 , 15976)
E_{12}	9633	334820	2 (27)	1	(9633 , 3357 , 14944)
E_{13}	9948	137203	5 (27)	-1	(9948 , -3675 , 14527)

Por último se ha desarrollado un método que permite determinar los cuatro cuerpos cúbicos contenidos en la composición de dos cuerpos cúbicos no conjugados de discriminante D. Aplicando dicho método se estudiaron las composiciones de los cuerpos cúbicos dados en la Tabla 3. Los resultados obtenidos constituyen la Tabla 4.

TABLA 4

Composición de los cuerpos cúbicos de discriminante $D = 188184253$

E_1, E_2, E_8, E_{12}	E_3, E_5, E_{10}, E_{12}
E_1, E_3, E_9, E_{13}	E_3, E_7, E_8, E_{11}
E_1, E_4, E_7, E_{10}	E_4, E_5, E_8, E_{13}
E_1, E_5, E_6, E_{11}	E_4, E_9, E_{11}, E_{12}
E_2, E_3, E_4, E_6	E_6, E_7, E_{12}, E_{13}
E_2, E_5, E_7, E_9	E_6, E_8, E_9, E_{10}
$E_2, E_{10}, E_{11}, E_{13}$	

3. SOBRE EL 3-RANGO DEL GRUPO DE IDEALES DE UN CUERPO CUADRATICO REAL DE DISCRIMINANTE PRIMO

La tabla de todos los cuerpos cúbicos de discriminante $D = p$ primo para $1 < p < 10^6$ es también la tabla de todos los cuerpos cuadráticos reales de discriminante primo p ($1 < p < 10^6$) tales que $r_3(p) \geq 1$ (es decir, tales que $3 \mid h(p)$) y para cada uno de ellos permite determinar $r_3(p)$ y $H_3(p)$. Un resumen estadístico de dicha tabla está dado en la siguiente

TABLA 5

Sector	P	P_1	P_2	δ_1	δ_2	$\delta_{2,1}$
$1 < p < 200000$	8984	1138	6	12.67	0.067	0.527
$1 < p < 400000$	16907	2199	12	13.01	0.071	0.546
$1 < p < 600000$	24534	3211	18	13.09	0.073	0.561
$1 < p < 800000$	31927	4229	26	13.25	0.081	0.615
$1 < p < 1000000$	39189	5269	30	13.45	0.077	0.569

donde: P = número de primos $p \equiv 1 \pmod 4$ en el sector
P_1 = número de primos p con $r_3(p) \geq 1$ en el sector
P_2 = número de primos con $r_3(p) \geq 2$ en el sector
$\delta_1 = (P_1/P) \cdot 100$
$\delta_2 = (P_2/P) \cdot 100$
$\delta_{2,1} = (P_2/P_1) \cdot 100$

Para los 608 primos p con $r_3(p) \geq 1$ del sector $1 < p < 10^5$ se calculó $h(p)$. La siguiente tabla da el número P_h de primos p en dicho sector con $h(p) = h$.

TABLA 6

h	3	9	15	21	27	33	39	45	51	57	63	87
P_h	507	63	18	7	4	2	1	2	1	1	1	1

El valor de $h(p)$ no se siguió calculando al enterarse el autor que dichos valores estaban incluídos en |7|. A pesar de ello se calculó $h(p)$ para los 30 primos $p < 10^6$ tales que $r_3(p) > 1$. Es claro que dichos primos son los dados en la Tabla 2 y que para todos ellos $r_3(p) = 2$.

TABLA 7

$h(p)$ para los primos p con $r_3(p) > 1$, $1 < p < 10^6$

p	$h(p)$	p	$h(p)$	p	$h(p)$
32009	9	321053	9	635909	27
62501	9	363397	9	686977	9
114889	9	412277	9	729293	9
142097	9	422573	9	775661	9
151141	9	449797	9	783689	27
153949	9	486221	9	785269	9
220217	9	529393	27	829813	9
255973	27	578581	9	893029	99
275881	9	602521	9	902333	9
282461	27	621749	9	946733	27

Los valores de $h(p)$ que aparecen en las dos últimas tablas nos permiten determinar inmediatamente la estructura de los correspondientes grupos $G(p)$. Siendo, además, $H_3(p) = H(p)$ si $h(p) = 3^m$, para algún entero $m > 0$, podemos concluir que la tabla hallada permite determinar el cuerpo de clases de Hilbert de 564 cuerpos cuadráticos reales de discriminante primo $p < 10^5$ y de todos los de la Tabla 7 con excepción de $p = 893029$. Tanto la estructura de $G(p)$ como $H(p)$ quedan determinadas para un gran número de primos $p < 10^6$ si se suman a nuestros resultados los obtenidos en [7].

Como parte de los resultados expuestos se tiene:

TEOREMA 3.1 *Existen 608 primos $p \equiv 1 \pmod 4$, $1 < p < 10^5$ tales que $3 \mid h(p)$, para todos ellos $G(p)$ es cíclico excepto para $p = 32009$ y $p = 62501$ para los cuales* $G(p) = Z_3 \oplus Z_3$.

TABLA 8

Primos $p \equiv 1 \pmod 4$, $1333333 < p < 9000000$ con más de un cuerpo cúbico de discriminante $D = p$ y $\delta = 1$, y el correspondiente $h(p)$. Para todos ellos $r_3(p) = 2$.

p	$h(p)$	p	$h(p)$	p	$h(p)$	p	$h(p)$
1375609	45	3008389	9	4902349	9	6974609	99
1419961	9	3030997	9	5020033	27	7038617	81
1495877	9	3034049	45	5025389	27	7066561	27
1536673	9	3057709	27	5048573	9	7080889	9
1595669	9	3081677	45	5119637	9	7086217	9
1658417	9	3085349	9	5180341	9	7145041	9
1659109	27	3089497	9	5183077	9	7234141	27
1697701	9	3108173	45	5195741	9	7274173	9
1717349	9	3143561	9	5322749	9	7343393	9
1766209	45	3295913	45	5370061	9	7443833	9
1777081	9	3505577	9	5373761	9	7481093	9
1783129	9	3525673	9	5387593	9	7491929	9
1789169	9	3636221	9	5622341	9	7601081	9
1791221	9	3743249	9	5701693	9	8003741	9
1874317	9	3799597	45	5709029	9	8070637	9
2042149	9	3870437	9	5748881	9	8072293	9
2043761	9	3948277	9	5754613	27	8197753	45
2097373	9	4024049	9	5858753	9	8213189	9
2178049	81	4073233	9	5880361	27	8260061	27
2185789	9	4261793	9	6204721	9	8343941	9
2357573	45	4386533	9	6270961	9	8355533	9
2772481	9	4405693	9	6272977	27	8388581	27
2803001	9	4453069	9	6469817	9	8554081	9
2853373	9	4515341	9	6753937	9	8711501	63
2906509	9	4531441	63	6775529	63	8826809	9
2922737	9	4784809	27	6876329	135	8881969	9

Ya hemos visto que si $r_3(p) > 2$ entonces $p > 1333333$. Observando el alto porcentaje de cuerpos con $\delta = 1$ en la Tabla 2 y que, según la Tabla 1, éstos corresponden a primos $p \equiv \pm 4 \pmod 9$, hemos elaborado una versión simplificada de RANG3: el programa RAPID que permite detectar aquellos primos $p \equiv \pm 4 \pmod 9$ para los cuales existen más de una terna de cuerpos cúbicos conjugados con $\delta = 1$. Es claro que para tales p, $r_3(p) > 1$. Así obtuvimos todos los p con esa propiedad para $1333333 < p < 9 \cdot 10^6$. Para cada uno de ellos calculamos $h(p) = 3^m \cdot m'$ $(3 \nmid m')$. Si $m = 2$ podemos asegurar que $r_3(p) = 2$. Para los restantes $(m > 2)$ utilizamos RANG3 y así concluímos que para todos ellos $r_3(p) = 2$. La Tabla 8 da los 104 primos p calculados y el correspondiente valor de $h(p)$. La estructura del correspondiente grupo $G(p)$ queda bien determinada para todos ellos excepto para los dos valores de p con $h(p) = 81$. El cuerpo de clases de Hilbert ha sido calculado para los 90 valores de p cuyo $h(p)$ es de la forma 3^m.

Por último, de los resultados expuestos (en particular de las tablas 3 y 4) podemos deducir:

TEOREMA 3.2 *Sea $p = 188184253$ y sea K el cuerpo cuadrático de discriminante p. Entonces el cuerpo de clases de Hilbert de K es $Q(\sqrt{p}, \alpha, \beta, \gamma)$* con

$$\alpha^3 = 370\alpha - 731 \quad , \quad \beta^3 = 604\beta - 5067 \quad y \quad \gamma^3 = 694\gamma - 6523 .$$

4. CONJETURAS

En esta sección final formularemos algunas conjeturas que nos han sido sugeridas por los resultados obtenidos en este trabajo.

En [6] se ha demostrado que existen infinitos cuerpos cuadráticos reales tales que $3 \mid h(D)$ (es decir, $r_3(D) \geq 1$). Este resultado puede reobtenerse fácilmente a partir de los nuestros. Sin embargo, los valores de δ_1 en la Tabla 5 nos permiten conjeturar un resultado mucho más fuerte:

Conjetura 1. El conjunto de los primos $p \equiv 1 \pmod 4$ tales que $r_3(p) \geq 1$ tiene densidad positiva.

Los resultados de la Tabla 6 y otros cálculos efectuados nos inducen a conjeturar que el conjunto de los primos $p \equiv 1 \pmod 4$ tales que $h(p) = 3$ también tiene densidad positiva. Estas conjeturas pueden ser mejor inducidas por los resultados de |7|. La imposibilidad de demostrar hasta el presente que existen infinitos D con $h(D) = 1$ (a pesar de los resultados numéricos) nos hacen pensar que aún no es posible decidir sobre conjeturas del tipo de las anteriores.

Vimos que hasta el presente se conocían pocos ejemplos de $D = p$ con $r_3(p) = 2$. Las dos últimas tablas dan 134 ejemplos y los cálculos efectuados nos llevan a conjeturar que existen infinitos primos $p \equiv 1 \pmod 4$ tales que $r_3(p) = 2$ (y hasta que dicho conjunto tiene densidad positiva si observamos el valor de δ_2 en la Tabla 5). En relación con ésto y observando que el 76.67% de los primos p de la Tabla 7 y el 73.08% de los primos p de la Tabla 8 tienen $h(p) = 9$, también conjeturamos que existen infinitos primos $p \equiv 1 \pmod 4$ tales que $G(p) \simeq Z_3 \oplus Z_3$.

Conjetura 2. Existen infinitos cuerpos cuadráticos reales cuyo grupo de clases de ideales es isomorfo a Z_3 e infinitos cuyo grupo de clases de ideales es isomorfo a $Z_3 \oplus Z_3$.

Por último, los cálculos efectuados nos hacen suponer que $D = 32009$ es el menor entero positivo tal que existen cuerpos cúbicos no cíclicos no conjugados de discriminante D y que si $p \equiv 1 \pmod 4$ es un primo tal que $r_3(p) > 2$ entonces $p > 9 \cdot 10^6$.

Addenda (enero 1982): Angel V. Oneto y el autor han generalizado el método expuesto en este trabajo. En efecto, en |10| desarrollan un método que permite determinar todos los cuerpos cúbicos que tienen un discriminante d dado y lo utilizan para construir la tabla de los 4753 cuerpos cúbicos reales no cíclicos con $d < 10^5$. De esta forma generalizan los resultados de |4| y completan los de |11| (ver |12|).

En particular se tiene que para $d = 22356$, 28212 y 31425 existen tres cuerpos cúbicos no cíclicos no conjugados de discriminante d. Estos son los únicos enteros positivos $d < 32009$ para los cuales existen cuerpos cúbicos no cíclicos no conjugados.

REFERENCIAS

1. BUELL,D.A.: *Class groups of quadratic fields*, Math. Comp. 30, (1976) pág. 610-623.

2. DELONE,B.N. and FADEEV,D.K.: *The Theory of Irrationalities of the Third Degree*, Transl. Math. Monog. A.M.S. Vol. X (1964).

3. DICKSON,L.E.: *Introduction to the Theory of Numbers*, University of Chicago Press (1929) (Dover, 1957).

4. GODWIN,H.J. and SAMET,P.A.: *A table of real cubic fields*, J. London Math. Soc. 34, (1959) pág. 108-110.

5. HERZ,C.S.: *Construction of class fields*, *Seminar on Complex Multiplication*, Lecture Notes in Math. 21 (1966) Exp. VII.

6. HONDA,T.: *On real quadratic fields whose class numbers are multiples of 3*, J. Reine. Angew. Math. 233, (1968), pág. 101-102.

7. LAKEIN,R.B.: *Review of UMT File. Table of class numbers, h(p) greater than 1, for fields* $Q(\sqrt{p})$, $p \equiv 1 \pmod 4 < 2776817$, Math. Comp. 29 (1975) pág. 335-336.

8. SHANKS,D.: *Class number, a theory of factorization, and genera*, Proc. Sym. Pure Math. XX, A.M.S. (1971), pág. 415-440.

9. SHANKS,D. and WEINBERGER,P.: *A quadratic field of primer discriminant requiring three generators for its class group, and related theory*, Acta Arithmetica, XXI (1972), pág. 71-87.

10. LLORENTE,P. y ONETO,A.V.: *Cuerpos cúbicos*, Cursos,Seminarios y Tesis del PEAM, nº 5, Univ. Zulia, Maracaibo, Venezuela, 1979.

11. ANGELL,I.O.: *A table of totally real cubic fields*, Math. Comp., 30 (1976), pág. 184-187

12. LLORENTE, P. y ONETO,A.V.: *On the real cubic fields*, Math. Comp. (en prensa).