MATHEMATICS OF COMPUTATION
VOLUME 49, NUMBER 180
OCTOBER 1987, PAGES 615-620

Calculation of the Class Numbers of Imaginary Cyclic Quartic Fields

By Kenneth Hardy,* R. H. Hudson,** D. Richman, Kenneth S. Williams,*** and N. M. Holtz

Abstract. Any imaginary cyclic quartic field can be expressed uniquely in the form $K = Q(\sqrt{A(D + B\sqrt{D})})$, where A is squarefree, odd and negative, $D = B^2 + C^2$ is squarefree, $B > 0$, $C > 0$, and $(A, D) = 1$. Explicit formulae for the discriminant and conductor of K are given in terms of A, B, C, D. The calculation of tables of the class numbers $h(K)$ of such fields K is described.

Let Q denote the field of rational numbers and let K be a cyclic extension of Q of degree 4. The unique quadratic subfield of K is denoted by k. The class number of K (resp. k) is denoted by $h(K)$ (resp. $h(k)$). The conductor of K is denoted by $f = f(K)$. In the case of *real* cyclic quartic fields K, Gras [3] has given a table of the values of $h(K)$ for all such fields with $f < 4000$. Recently, the authors have carried out the calculation of the class numbers of *imaginary* cyclic quartic fields [4]. In this note we give a brief description of the computation of the tables given in [4].

The following explicit representation of a cyclic quartic field is proved in [4, Theorem 1].

THEOREM 1. *If K is a real or imaginary cyclic quartic extension of Q, then there are integers A, B, C, D such that*

$$K = Q\left(\sqrt{A(D + B\sqrt{D})}\right) = Q\left(\sqrt{A(D - B\sqrt{D})}\right), \tag{1}$$

where

$$\begin{cases} A \text{ is squarefree and odd}, \\ D = B^2 + C^2 \text{ is squarefree}, \ B > 0, \ C > 0, \\ A \text{ and } D \text{ are relatively prime}. \end{cases} \tag{2}$$

Moreover, any field satisfying (1) and (2) is a cyclic quartic extension of Q. The representation of K in (1) is unique in the sense that if $K = Q(\sqrt{A_1(D_1 + B_1\sqrt{D_1})})$ is another representation of K, where A_1, B_1, C_1, D_1 are integers satisfying the conditions of (2), then $D = D_1$, $A = A_1$, $B = B_1$, $C = C_1$.

Received November 10, 1986.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11R29, 11R16; Secondary 11R20.
Key words and phrases. Imaginary cyclic quartic fields, class number, discriminant.
*Research supported by Natural Sciences and Engineering Research Council of Canada Grant A-7823.
**Research supported in part by a research grant from the University of South Carolina.
***Research supported by Natural Sciences and Engineering Research Council of Canada Grant A-7233.

0025-5718/87 $1.00 + $.25 per page

We remark that the field K is totally real if $A > 0$, and is totally imaginary if $A < 0$.

Next we let G denote the multiplicative group of residues coprime with $f = f(K)$, so that $G \simeq \mathrm{Gal}(Q(e^{2\pi i/f})/Q)$. The subgroup of G which is isomorphic to $\mathrm{Gal}(Q(e^{2\pi i/f})/K)$ is denoted by H. H is a subgroup of index 4 in G and the factor group G/H is cyclic of order 4. Let α be an element of G such that G/H is generated by αH. We define a character χ on G by

$$\chi(\alpha) = i, \qquad \chi(h) = 1 \quad \text{for all } h \in H. \tag{3}$$

The character χ is a quartic, primitive, odd character of conductor f.

When K is taken to be an imaginary cyclic quartic field, the class number formula for Abelian fields yields the following formula for $h(K)$ [4, Theorem 3].

THEOREM 2. *If K is an imaginary cyclic quartic field of conductor f with quadratic subfield k, then*

$$h(K) = \rho h(k) \left| \sum_{0<n<f/2} \chi(n) \right|^2, \tag{4}$$

where the value of the quantity ρ is given by

$$\rho = \begin{cases} 1/2, & \text{if } f = 5, \\ 1/8, & \text{if } f > 5,\ f \text{ even}, \\ 1/2, & \text{if } f > 5,\ f \text{ odd},\ \chi(2) = 1, \\ 1/18, & \text{if } f > 5,\ f \text{ odd},\ \chi(2) = -1, \\ 1/10, & \text{if } f > 5,\ f \text{ odd},\ \chi(2) = \pm i, \end{cases} \tag{5}$$

and χ is defined in (3).

In order to use Theorem 2 to calculate $h(K)$, we need to be able to compute f. A formula for f in terms of D, A, B, C is given in Theorem 3 (see [4, Theorem 5]).

THEOREM 3. *The conductor $f(K)$ of the (real or imaginary) cyclic quartic field $K = Q(\sqrt{A(D + B\sqrt{D})})$, where A is squarefree and odd, $D = B^2 + C^2$ is squarefree, $B > 0$, $C > 0$, and $(A, D) = 1$, is given by*

$$f(K) = 2^l |A| D, \tag{6}$$

where

$$l = \begin{cases} 3, & \text{if } D \equiv 2 \pmod 8, \\ & \text{or} \\ & D \equiv 1 \pmod 4,\ B \equiv 1 \pmod 2, \\ 2, & \text{if } D \equiv 1 \pmod 4,\ B \equiv 0 \pmod 2,\ A + B \equiv 3 \pmod 4, \\ 0, & \text{if } D \equiv 1 \pmod 4,\ B \equiv 0 \pmod 2,\ A + B \equiv 1 \pmod 4. \end{cases} \tag{7}$$

Also, in order to apply (4), it is necessary to be able to compute $\chi(g)$ for $g \in G$. Since $g = \alpha^i h$ for some $i = 0, 1, 2, 3$ and some $h \in H$, it suffices to have a criterion for recognizing when an element of G is actually in H. As each element of G is congruent to a prime modulo f, we can test whether g belongs to H or not by means of the following theorem [4, Theorem 6].

THEOREM 4. *Let K be a (real or imaginary) cyclic quartic field $Q(\sqrt{A(D+B\sqrt{D})})$, where A is squarefree and odd, $D = B^2 + C^2$ is squarefree, $B > 0$, $C > 0$, and $(A, D) = 1$. Let H be the subgroup of the multiplicative group of residues coprime with $f = f(K)$ which is isomorphic to $\mathrm{Gal}(Q(e^{2\pi i/f})/K)$. Let p be an odd prime not dividing A, B, C or D. Then $p \in H$ if and only if*

$$\left(\frac{D}{p}\right) = +1, \qquad \left(\frac{A(D+BE)}{p}\right) = +1, \tag{8}$$

where $D \equiv E^2 \pmod p$ and $(\frac{\ }{p})$ denotes Legendre's symbol of quadratic residuacity $\pmod p$.

From now on, we restrict K to be an *imaginary* cyclic quartic field, so that in the representation (1) we have $A < 0$. Theorems 1, 2, 3, 4 were used to calculate the class numbers $h(K)$ of the 3521 distinct fields K with

$$1 < D < 1000, \qquad 1 \leqslant -A < 20, \tag{9}$$

as well as those of the 4274 fields with conductor f satisfying

$$f < 10{,}000. \tag{10}$$

The calculations were carried out using computer programs written in PASCAL and implemented on both an IBM micro computer and an APOLLO mini computer. The resulting values are listed in the tables in [4].

We just list at the end of this note the values of $h(K)$ for those fields K with $f \leqslant 200$.

We now describe briefly how the computation of $h(K)$ was carried out. First, Theorem 3 was used to generate two data files containing the values of (D, A, B, C) and f: one for the fields K specified by (9), the other for those fields given by (10). For each of these two data files, a file of the class numbers $h(K)$ was produced as follows.

For each (D, A, B, C) an element α of G was determined such that $G/H = \langle \alpha H \rangle$. This was done by finding a small integer k coprime with f for which the least prime $p \equiv k^2 \pmod f$ satisfied

$$\left(\frac{D}{p}\right) = -1, \quad \text{or} \quad \left(\frac{D}{p}\right) = +1 \ (\text{say } D \equiv E^2 (\mathrm{mod}\, p)) \quad \text{and} \quad \left(\frac{A(D+BE)}{p}\right) = -1. \tag{11}$$

By Theorem 4 we see that $p \notin H$. As $|G/H| = 4$, we have $(kH)^4 = H$. Clearly, $(kH)^2 \neq H$, for otherwise we would have $k^2 \in H$, contradicting $p \notin H$. Hence, $\mathrm{ord}_{G/H}(kH) = 4$ and so we may take $\alpha = k$.

Next, for each (D, A, B, C), a set of elements from which the subgroup H is easily constructed, was found. This was done by determining the generators of the cyclic groups of prime power order in the decomposition of G as described, for example, in [1]. These generators were stored together with their orders. The generators of the odd part of G are also the generators of the odd part of H. For each generator g_i $(i = 1, 2, \ldots, s)$ of the 2-part of G, the unique integer $j(g_i)$ $(= 0, 1, 2, 3)$ was determined such that $g_i \in \alpha^{j(g_i)} H$, using the value of α calculated above and the criterion of Theorem 4. The values of $j(g_i)$ were stored. The 2-part of H is given by

the elements

$$g_1^{x_1} \cdots g_s^{x_s} \qquad (0 \leqslant x_i \leqslant \operatorname{ord}(g_i) - 1, 1 \leqslant i \leqslant s) \tag{12}$$

for which

$$x_1 j(g_1) + \cdots + x_s j(g_s) \equiv 0 \pmod 4. \tag{13}$$

Then, for each (D, A, B, C), the value of $|\Sigma_{0<n<f/2} \chi(n)|^2$ was calculated by means of the equation

$$\left| \sum_{0<n<f/2} \chi(n) \right|^2 = (C_0 - C_2)^2 + (C_1 - C_3)^2, \tag{14}$$

where

$$C_r = \sum_{\substack{0<n<f/2 \\ n \in \alpha^r H}} 1 \qquad (r = 0, 1, 2, 3). \tag{15}$$

The identities

$$C_0 + C_2 = \phi(f)/4, \qquad C_1 + C_3 = \phi(f)/4 \tag{16}$$

served as checks on the calculation.

As the relative class number $h(K)/h(k)$ is an integer, the following congruence holds (see Theorem 2):

$$(C_0 - C_2)^2 + (C_1 - C_3)^2 \equiv 0 \pmod t, \tag{17}$$

where

$$t = \begin{cases} 8, & \text{if } f > 5,\ f \text{ even}, \\ 18, & \text{if } f > 5,\ f \text{ odd},\ \chi(2) = -1, \\ 10, & \text{if } f > 5, f \text{ odd},\ \chi(2) = \pm i, \\ 2, & \text{otherwise.} \end{cases} \tag{18}$$

This congruence was used as another check on the calculation, in order to reduce the chances of a computer error.

Finally, Theorem 2 was used to calculate $h(K)$ from the values of $(C_0 - C_2)^2 + (C_1 - C_3)^2$, the values of $h(k)$ given in [6], and the values of ρ defined by (5).

When $D = q$ (prime) $= a^2 + b^2 \equiv 5 \pmod 8$, $q < 1000$, $A = -1$, $B = b \equiv 0 \pmod 2$, $C = a \equiv 1 \pmod 2$, our values agree with those in [5]. In addition, when $D = 5$, our values agree with those which can be deduced from the table in [2].

The following table is a very short extract taken from the second table in [4].

Table of class numbers of imaginary cyclic quartic fields

$$Q\left(\sqrt{A(D + B\sqrt{D})}\right),$$

where D, A, B, C *are integers such that*

A *is squarefree, odd, and negative,*

$D = B^2 + C^2$ *is squarefree,* $B > 0$, $C > 0$,

$(A, D) = 1$

in the range

$$f < 200.$$

case	f	D	$-A$	B	C	$h(k)$	$h(K)$
1	5	5	1	2	1	1	1
2	13	13	1	2	3	1	1
3	16	2	1	1	1	1	1
4	29	29	1	2	5	1	1
5	37	37	1	6	1	1	1
6	40	5	1	1	2	1	2
7	48	2	3	1	1	1	2
8	51	17	3	4	1	1	10
9	53	53	1	2	7	1	1
10	60	5	3	2	1	1	4
11	61	61	1	6	5	1	1
12	65	5	13	2	1	1	2
13	65	13	5	2	3	1	2
14	68	17	1	4	1	1	4
15	80	2	5	1	1	1	2
16	80	10	1	1	3	2	20
17	80	10	1	3	1	2	4
18	85	5	17	2	1	1	2
19	85	85	1	2	9	2	20
20	85	85	1	6	7	2	4
21	101	101	1	10	1	1	5
22	104	13	1	3	2	1	2
23	105	5	21	2	1	1	4
24	109	109	1	10	3	1	17
25	112	2	7	1	1	1	4
26	119	17	7	4	1	1	2
27	120	5	3	1	2	1	4
28	123	41	3	4	5	1	34
29	136	17	1	1	4	1	4
30	140	5	7	2	1	1	4
31	145	5	29	2	1	1	4
32	145	29	5	2	5	1	4
33	149	149	1	10	7	1	9
34	156	13	3	2	3	1	8
35	157	157	1	6	11	1	5
36	164	41	1	4	5	1	4
37	165	5	33	2	1	1	8
38	173	173	1	2	13	1	5
39	176	2	11	1	1	1	10
40	181	181	1	10	9	1	25
41	185	5	37	2	1	1	10
42	185	37	5	6	1	1	10
43	187	17	11	4	1	1	34
44	195	65	3	8	1	2	8
45	195	65	3	4	7	2	104
46	197	197	1	14	1	1	5

K. Hardy and K. S. Williams
Department of Mathematics and Statistics
Carleton University
Ottawa, Ontario, Canada K1S 5B6

R. H. Hudson and D. Richman
Department of Mathematics
University of South Carolina
Columbia, South Carolina 29208

N. M. Holtz
Department of Civil Engineering
Carleton University
Ottawa, Ontario, Canada K1S 5B6

1. E. D. BOLKER, *Elementary Number Theory*, Benjamin, New York, 1970.

2. HARVEY COHN, "A computation of some bi-quadratic class numbers," *MTAC*, v. 12, 1958, pp. 213–217.

3. M.-N. GRAS, *Table Numérique du Nombre de Classes et des Unités des Extensions Cycliques Réelles de Degré* 4 *de Q*, Publ. Math. Univ. Besançon, 1977/78, fasc. 2, 53 pp.

4. K. HARDY, R. H. HUDSON, D. RICHMAN, K. S. WILLIAMS & N. M. HOLTZ, *Calculation of the Class Numbers of Imaginary Cyclic Quartic Fields*, Carleton–Ottawa Mathematical Lecture Note Series, No. 7, July 1986, 201 pp.

5. R. H. HUDSON & K. S. WILLIAMS, *A Class Number Formula for Certain Quartic Fields*, Carleton Mathematical Series No. 174, February 1981, 25 pp.

6. B. ORIAT, *Groupe des Classes des Corps Quadratiques Réels* $Q(\sqrt{d})$, $d < 10000$, Faculté des Sciences de Besançon, Besançon, France, 53 pp.