PROCEEDINGS

of the

INTERNATIONAL CONFERENCE

on

CLASS NUMBERS AND FUNDAMENTAL UNITS

of

ALGEBRAIC NUMBER FIELDS

JUNE 24 – 28, 1986

KATATA, JAPAN

CALCULATION OF THE CLASS NUMBERS OF CERTAIN QUARTIC FIELDS

Kenneth S. Williams
Department of Mathematics and Statistics
Carleton University, Ottawa, Ontario, Canada

0. Acknowledgement. This talk describes joint work with Professors K. Hardy and N.M. Holtz of Carleton University, Ottawa, Ontario, Canada and Professors R.H. Hudson and D. Richman of the University of South Carolina, Columbia, South Carolina, U.S.A.

1. Introduction. Let Q denote the field of rational numbers and let K be a cyclic extension of Q of degree 4. The unique (real) quadratic subfield of K is denoted by k. The class number of K (respectively k) is denoted by $h(K)$ (respectively $h(k)$). Tables of the class numbers of real cyclic quartic fields have been given by Gras [6]. In this talk we describe the calculation of tables of $h(K)$ for imaginary cyclic quartic fields K.

2. Cyclic quartic fields. In 1980 Edgar and Peterson [5] showed that every cyclic quartic extension of Q can be expressed in the form

$$K = Q\left(\sqrt{rd + p\sqrt{d}}\right),$$

where d is a squarefree integer > 1 and p, q, r are nonzero integers such that

$$r^2 d = p^2 + q^2.$$

In fact one can always choose (p, q, r) so that r divides p, and so K can be represented in the form

$$\begin{cases} K = Q\left(\sqrt{a(d + b\sqrt{d})}\right), \\ d = b^2 + c^2 \text{ squarefree}, b > 0, c > 0, \\ a \text{ squarefree}. \end{cases}$$

This representation of K is more convenient than Edgar and Peterson's but has the disadvantage of not being unique. For example we have

$$Q\left(\sqrt{-(5+\sqrt{5})}\right) = Q\left(\sqrt{-2(5+2\sqrt{5})}\right).$$

In view of the identity

$$Q\left(\sqrt{a(d+b\sqrt{d})}\right) = Q\left(\sqrt{(a/2)(d+c\sqrt{d})}\right)$$

we can clearly take a to be odd. Moreover a and d can be taken to be coprime. This is proved in [7: Theorem 1]. Thus we have the following result.

THEOREM 1. Any cyclic quartic field K can be written in the form

$$K = Q\left(\sqrt{A(D+B\sqrt{D})}\right), \tag{2.1}$$

where

$$\begin{cases} A \text{ is squarefree and odd,} \\ D = B^2 + C^2 \text{ is squarefree, } B > 0, C > 0, \\ (A, D) = 1. \end{cases} \tag{2.2}$$

Throughout the rest of this talk it is assumed that K is taken in this form. Further, it is proved in [7: Theorem 1] that this representation of K is unique in the sense that if $K = Q\left(\sqrt{A_1(D_1+B_1\sqrt{D_1})}\right)$ is another representation of K, where A_1, B_1, C_1, D_1, also satisfy the conditions (2.2), then $D = D_1, A = A_1$, $B = B_1, C = C_1$. We remark that the field K is real if $A > 0$ and is imaginary if $A < 0$.

3. Class number formula for $h(K)$. Throughout this section we assume that K is an imaginary cyclic quartic field so that in the representation of K given in (2.1) we have $A < 0$. As K is totally complex, $\theta = \sqrt{A(D+B\sqrt{D})}$ has $r_1 = 0$ real conjugates and $2r_2 = 4$ imaginary conjugates. Hence, by Dirichlet's unit theorem, since $r_1 + r_2 - 1 = 1$, K has a single fundamental unit. Hasse [8] has noted that this unit may be taken to be the fundamental unit $\varepsilon(> 1)$ of $k = Q(\sqrt{D})$. Thus the regulator $r(K)$ of K is given by

$$r(K) = 2\log\varepsilon. \tag{3.1}$$

Hasse [8] has also observed that the only roots of unity in K are ± 1 except for the exceptional field

$$K = Q\left(\sqrt{-(5+2\sqrt{5})}\right) = Q\left(e^{2\pi i/5}\right),$$

which contains the additional roots of unity

$$\pm e^{2\pi m i/5} (m = 1, 2, 3, 4).$$

Thus, the number $w(K)$ of roots of unity in K, is given by

$$w(K) = \begin{cases} 2, & \text{if } K \neq Q(e^{2\pi i/5}), \\ 10, & \text{if } K = Q(e^{2\pi i/5}). \end{cases} \tag{3.2}$$

As K is an abelian field, by the Kronecker-Weber theorem, there is a positive integer f such that

$$K \subseteq Q(e^{2\pi i/f}). \tag{3.3}$$

The least such positive integer f is called the conductor of K and is denoted by $f = f(K)$. Clearly we can rewrite (3.2) in the form

$$w(K) = \begin{cases} 2, & \text{if } f > 5, \\ 10, & \text{if } f = 5. \end{cases} \tag{3.4}$$

The conductor of the field k is denoted by $m = f(k)$. Since k is the quadratic field $Q(\sqrt{D})$, it is well-known that

$$m = \begin{cases} D, & \text{if } D \equiv 1 \pmod 4, \\ 4D, & \text{if } D \equiv 0 \pmod 4. \end{cases} \tag{3.5}$$

By the conductor-discriminant formula, the discriminant $d(K)$ of the field K is related to m and f by the relation

$$d(K) = mf^2. \tag{3.6}$$

Next we let G denote the multiplicative group of residues which are coprime with f. The group G is isomorphic in a natural way to $\mathrm{Gal}(Q(e^{2\pi i/f})/Q)$. We denote by H the subgroup of G which is isomorphic to $\mathrm{Gal}(Q(e^{2\pi i/f})/K)$. By galois theory we know that G/H is a cyclic group of order 4. We let α be an element of G such that

$$G/H = < \alpha H > . \tag{3.7}$$

The particular choice of α will not be important in what we do. We define a character χ on G (χ depends on the choice of α) by

$$\chi(\alpha) = i, \quad \chi(h) = 1 \quad (\forall h \in H). \tag{3.8}$$

χ is a quartic, primitive, odd character of conductor f which is trivial on H. All the characters on G which are trivial on H are given by

$$\chi_0, \chi, \chi^2, \chi^3, \tag{3.9}$$

where $\chi^4 = \chi_0$ (the trivial character on G). The character $\chi^3 = \bar{\chi}$ is also a quartic, primitive, odd character of conductor f. However, the character χ^2 may not be primitive. The primitive character $(\chi^2)'$ induced by χ^2 is given by

$$(\chi^2)'(n) = \left(\frac{m}{n}\right), \quad (n,m) = 1, \tag{3.10}$$

where $\left(\frac{m}{n}\right)$ is the Jacobi symbol of conductor m.

In order to apply the class number formula for abelian fields to K, we will need the product

$$\Pi_{r=1}^{3} L(1, (\chi^r)'),$$

where

$$L(1,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n}.$$

Berndt [1] has shown that

$$L(1,\chi) = \frac{\pi \sum_{0<n<f/2} \bar{\chi}(n)}{iG(\bar{\chi})(\chi(2)-2)}, \tag{3.11}$$

where the Gauss sum $G(\chi)$ is given by

$$G(X) = \sum_{j=1}^{f} \chi(j) e^{2\pi i j/f}. \tag{3.12}$$

It is a well-known property of Gauss sums that

$$G(\chi)G(\bar{\chi}) = -G(\chi)\overline{G(\chi)} = -\,|\,G(\chi)\,|^2 = -f, \tag{3.13}$$

and so

$$L(1,\chi)L(1,\chi^3) = \frac{\pi^2}{f(\chi(2)-2)(\bar{\chi}(2)-2)}\left|\sum_{0<n<f/2}\chi(n)\right|^2. \tag{3.14}$$

Further, by Dirichlet's class number formula for $k = Q(\sqrt{D})$, we have

$$L(1,(\chi^2)') = \sum_{n=1}^{\infty}\frac{\left(\frac{m}{n}\right)}{n} = \frac{2h(k)\log\varepsilon}{\sqrt{m}}. \tag{3.15}$$

Hence we obtain

$$\Pi_{r=1}^{3}L(1,(\chi^r)') = \frac{2\pi^2 h(k)\log\varepsilon}{\sqrt{m}f(\chi(2)-2)(\bar{\chi}(2)-2)}\left|\sum_{0<n<f/2}\chi(n)\right|^2. \tag{3.16}$$

Now, for any abelian extension L of Q, the class number formula for $h(L)$ asserts that (see for example [11])

$$h(L) = \frac{w(L)\mid d(L)\mid^{1/2}}{2^{r_1+r_2}\pi^{r_2}r(L)}\prod_{\substack{\chi\neq\chi_0\\ \chi|_H=1}}L(1,\chi'). \tag{3.17}$$

Appealing to (3.1), (3.4), (3.5), (3.6), (3.16), we obtain

$$h(K) = \rho h(k)\mid\sum_{0<n<f/2}\chi(n)\mid^2, \tag{3.18}$$

where

$$\rho = \begin{cases} 1/2, & \text{if } f=5 \text{ or } f>5, f \text{ odd}, \chi(2)=1,\\ 1/8, & \text{if } f>5, f \text{ odd}, \chi(2)=-1,\\ 1/10, & \text{if } f>5, f \text{ odd}, \chi(2)=\pm i,\\ 1/8, & \text{if } f>5, f \text{ even}. \end{cases} \tag{3.19}$$

Setting

$$C_i = \sum_{\substack{0<n<f/2\\ n\in\alpha^i H}} 1 \quad (i=0,1,2,3) \tag{3.20}$$

the equation (3.18) becomes

$$h(K) = \rho h(k)\left((C_0-C_2)^2+(C_1-C_3)^2\right). \tag{3.21}$$

In order to use (3.21) to calculate $h(K)$ numerically we require:

(i) an explicit formula for f,

(ii) a test to decide whether an element of G belongs to H or not,

(iii) a way of calculating α,

(iv) tables of $h(k)$.

In section 4 we give an explicit formula for f. In section 5 we give a test which enables us to determine whether an element of G is in H or not. This is used in section 6 to show how to calculate α. Tables of $h(k)$ are readily available (for example [12]).

4. Explicit formula for the conductor f. In this section the field K can be real or imaginary. The minimal polynomial of

$$\theta = \sqrt{A(D + B\sqrt{D})} \tag{4.1}$$

is

$$f(X) = X^4 - 2ADX^2 + A^2C^2D \tag{4.2}$$

so that

$$\text{discrim } (f(X)) = 2^8 A^6 B^4 C^2 D^3. \tag{4.3}$$

Since $d(K)$ divides discrim $(f(X))$ this shows that the only possible primes dividing $d(K)$ are 2 and the primes dividing $ABCD$. It follows from a theorem of Llorente, Nart and Vila [10] that, in the case of odd primes p, we have

$$p^{2\alpha+3\delta} \parallel d(K), \tag{4.4}$$

where

$$p^\alpha \parallel A, p^\delta \parallel D. \tag{4.5}$$

When $p = 2$ the theorem of Llorente, Nart and Vila does not apply. Instead, proceeding 2-adically, we show that (see [7]),

$$2^e \parallel d(K), \tag{4.6}$$

where

$$e = \begin{cases} 8, & \text{if } D \equiv 2 \pmod 8, \\ 6, & \text{if } D \equiv 1 \pmod 4,\ B \equiv 1 \pmod 2, \\ 4, & \text{if } D \equiv 1 \pmod 4,\ B \equiv 0 \pmod 2,\ A+B \equiv 3 \pmod 4, \\ 0, & \text{if } D \equiv 1 \pmod 4,\ B \equiv 0 \pmod 2,\ A+B \equiv 1 \pmod 4. \end{cases} \tag{4.7}$$

This proves that

$$d(K) = 2^e A^2 D^3, \tag{4.8}$$

where e is given in (4.7). Appealing to (3.5), (3.6) and (4.8), we obtain

THEOREM 2. If

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

where A, B, C, D satisfy (1.2), then

$$f(K) = 2^{\ell} \mid A \mid D, \tag{4.9}$$

where

$$\ell = \begin{cases} 3, & \text{if } D \equiv 2 \pmod 8 \text{ or } D \equiv 1 \pmod 4,\ B \equiv 1 \pmod 2, \\ 2, & \text{if } D \equiv 1 \pmod 4,\ B \equiv 0 \pmod 2,\ A+B \equiv 3 \pmod 4, \\ 0, & \text{if } D \equiv 1 \pmod 4,\ B \equiv 0 \pmod 2,\ A+B \equiv 1 \pmod 4. \end{cases} \tag{4.10}$$

5. Test to decide whether an element $g \in G$ is in H or not. In this section K can be a real or imaginary field. Let $g \in G$ so that g is an integer coprime with f. By Dirichlet's theorem, we can find a prime $p \equiv g \pmod f$. Moreover p can always be choosen so that $p \nmid 2ABCD$. This guarantees that $p \nmid f$ and $p \nmid \text{discrim}\,(f(X))$. It follows from galois theory that

(5.1) $g \in H \Leftrightarrow p \epsilon H \Leftrightarrow f(X)$ splits completely into linear factors (mod p).

Appealing to a theorem of Carlitz [3], $f(X)$ is the product of 4 linear factors (mod p) if and only if

$$\left(\frac{D}{p}\right) = \left(\frac{A(D+BE)}{p}\right) = 1, \tag{5.2}$$

where

$$D \equiv E^2 \pmod p. \tag{5.3}$$

This provides us with the required test.

6. Calculation of α. In this section K can be a real or imaginary field. We may determine α as follows. We determine the least integer α coprime with f for which there is a prime p (not dividing $2ABCD$) such that

$$(6.1) \qquad \begin{cases} p \equiv \alpha^2 \pmod{f}, \\ \left(\frac{D}{p}\right) = -1 \text{ or } \left(\frac{D}{p}\right) = +1, \left(\frac{A(D+BE)}{p}\right) = -1, \text{ where } D \equiv E^2 \pmod{p}. \end{cases}$$

Clearly, as $(\alpha, f) = 1$ we have $(p, f) = 1$, so that $p \in G$. Moreover, by the test in section 5, we see that $p \notin H$, and so $\alpha^2 \notin H$. Hence $H, \alpha H, \alpha^2 H, \alpha^3 H$ are distinct cosets and we have $G/H =< \alpha H >$ as required.

7. Method of calculation of $h(K)$. Let K be the imaginary cyclic quartic field $Q\left(\sqrt{A(D + B\sqrt{D})}\right)$, where $A < 0$ is squarefree and odd, $D = B^2+C^2$ is squarefree $(B > 0, C > 0)$ and $(A, D) = 1$. Using the results mentioned above we calculated the class numbers $h(K)$ of the 3521 distinct fields K with

$$(7.1) \qquad 1 < D < 1000, \quad 1 \leq -A \leq 20,$$

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

$$(7.2) \qquad f < 10{,}000.$$

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 [7].

We now describe briefly how the computations were carried out. First, Theorem 2 was used to generate two data files containing the values of (D, A, B, C) and f: one for the fields K specified by (7.1), the other for those fields given by (7.2). 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 $G/H =< \alpha H >$. This was done by the method described in section 6. 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 [2]. 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 $g_i (i = 1, 2, \cdots, s)$ 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 section 5. The values of $j(g_i)$ were stored. The 2-part of H is given by the elements

$$g_1^{x_1} \cdots g_s^{x_s} (0 \leq x_i \leq \text{ord}(g_i) - 1, \quad 1 \leq i \leq s) \tag{7.3}$$

for which

$$x_1 j(g_1) + \cdots + x_s j(g_s) \equiv 0 \pmod 4. \tag{7.4}$$

Then, for each (D, A, B, C), the value of

$$(C_0 - C_2)^2 + (C_1 - C_3)^2,$$

where C_i is defined in (3.20), was calculated.

The identities

$$C_0 + C_2 = \phi(f)/4, \quad C_1 + C_3 = \phi(f)/4 \tag{7.5}$$

served as checks on the calculation.

As the relative class number $h(K)/h(k)$ is an integer the following congruence holds

$$(C_0 - C_2)^2 + (C_1 - C_3)^2 \equiv 0 \pmod{\text{t}}, \tag{7.6}$$

where

$$t = \begin{cases} 8, & \text{if } f > 5, f \text{ even}, \\ 18, & \text{if } f > 5, f \text{ odd}, \chi(2) = -1, \\ 10, & \text{if } f > 5, f \text{ odd}, \chi(2) = \pm i, \\ 2, & \text{otherwise.} \end{cases} \tag{7.7}$$

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

Finally, (3.21) was used to calculate $h(K)$ from the values of $(C_0 - C_2)^2 + (C_1 - C_2)^2$, the values of $h(k)$ given in [12], and the values of ρ defined by (3.19).

When $D = q(\text{prime}) = a^2 + b^2 \equiv 5 \pmod 8$, $q < 1000, A = -1$, $B = b \equiv 0 \pmod 2$, $C = a \equiv 1 \pmod 2$, our values agree with those in [9]. In addition when $D = 5$ our values agree with those which can be deduced from the table in [4].

8. 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 and odd, $A < 0$

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

$(A, D) = 1$

in the range

$$f < 200.$$

This is an extract from the table in [7] for $f < 10,000$.

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

9. References.

1. B.C. Berndt, Classical theorems on quadratic residues, Enseign. Math. 22 (1976), 261-304.

2. E.D. Bolker, Elementary Number Theory, W.A. Benjamin, Inc. New York (1970).

3. L. Carlitz, Note on a quartic congruence, Amer. Math. Monthly 63 (1956), 569-571.

4. Harvey Cohn, A computation of some bi-quadratic class numbers, Mathematical Tables and other Aids to Computing 12 (1958), 213-217.

5. H. Edgar and B. Peterson, Some contributions to the theory of cyclic quartic extensions of the rationals, J. Number Theory 12 (1980), 77-83.

6. M.-N. Gras, Table numérique du nombre de classes et des unités des extensions cycliques réelles de degré 4 de Q, Publ. Math. Univ. Besancon, 1977/78, fasc. 2, 53 pp.

7. K. Hardy, R.H. Hudson, D. Richman, K.S. Williams and N.M. Holtz, Calculation of the class numbers of imaginary cyclic quartic fields, Carleton-Ottawa Mathematical Lecture Notes Series No. 7, July 1986, 201 pp.

8. H. Hasse, Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern, Akademie-Verlag Berlin (1950).

9. R.H. Hudson and K.S. Williams, A class number formula for certain quartic fields, Carleton Mathematical Series No. 174, February 1981, 25pp.

10. P. Llorente, E. Nart and N. Vila, Discriminants of number fields defined by trinomials, Acta Arith. 43 (1984), 367-373.

11. W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, Polish Scientific Publishers, Warsaw (1974).

12. B. Oriat, Groupe des classes des corps quadratiques réels $Q(\sqrt{d})$, $d < 10000$, Facultés des Sciences de Besancon, Besancon, France, 53pp.