数理解析研究所講究録
第 603 巻 1987 年 51-59

THE CLASS NUMBER TWO PROBLEM FOR CERTAIN QUARTIC FIELDS

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

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

1. Introduction. Let K denote an algebraic number field of finite degree over the rational field Q. The ring of integers of K is denoted by O_K. If A and B are nonzero ideals of O_K, we say that A is equivalent to B, written $A \sim B$, if there exist nonzero elements α and β of O_K such that $(\alpha)A = (\beta)B$. It is easy to check that $\sim$ is an equivalence relation and it is a classical result that the number of equivalence classes is finite. The number of equivalence classes is called the classnumber of K and is denoted by $h(K)$.

It is a result going back to Dedekind that $h(K) = 1$ if and only if O_K is a unique factorization domain. More recently Carlitz [5] has shown that $h(K) = 2$ if and only if O_K is not a unique factorization domain but every factorization of a nonzero, nonunit integer of K contains the same number of primes. It is thus of interest to determine those algebraic number fields K having $h(K) = 1$ or $h(K) = 2$. However this is an extremely difficult problem. Even if K is restricted to a certain class of fields, such as quadratic fields, the problem is still difficult.

The first results of this type were obtained by Stark [11] in 1967 who showed that there are exactly nine imaginary quadratic fields $K = Q(\sqrt{d})$ ($d < 0, d$ squarefree) with classnumber 1, namely those for which $d = -1, -2, -3, -7, -11, -19, -43, -67$ or -163. The determination of all imaginary quadratic fields $K = Q(\sqrt{d})$ ($d < 0, d$ squarefree) with $h(K) = 2$ was carried out by Baker [1] and Stark [12] in 1971. They proved that

$$\begin{aligned} h(K) = 2 \Leftrightarrow d = &-5, -6, -10, -15, -22, -35, -37 \\ &-51, -52, -58, -91, -115, -123, \\ &-187, -235, -267, -403, -427. \end{aligned}$$

More recently Mestre [9] has shown that if $-d$ is prime then

$$h(Q(\sqrt{d})) > \frac{1}{55} \log \mid d \mid,$$

with a similar inequality when $-d$ is composite. These inequalities allow in principle the determination of all imaginary quadratic fields $K = Q(\sqrt{d})$ $(d < 0, d$ squarefree) having $h(K) \leq 100$. There are 16 imaginary quadratic fields with $h(K) = 3$ and 54 fields with $h(K) = 4$. These results for imaginary quadratic fields contrast sharply with the case when $k = Q(\sqrt{d})$ is a real quadratic field. It was conjectured by Gauss that there are infinitely many real quadratic fields K for which $h(K) = 1$ but it is still not known whether this is true or false.

In the case of imaginary bicyclic quartic fields $K = Q(\sqrt{d_1}, \sqrt{d_2})$, Brown and Parry [3] showed in 1974 that $h(K) = 1$ if and only if K belongs to a list of 47 fields. In 1977 Buell, Williams and Williams [4] showed that $h(K) = 2$ if and only if K belongs to a list of 160 fields, provided the known list of imaginary quadratic fields with classnumber 4 is complete. Since this list is now known to be complete from the work of Mestre mentioned above, the list of 160 imaginary bicyclic quartic fields of classnumber 2 is also complete.

In the case of imaginary cyclic quartic fields K, Uchida [13] showed in 1972 that if the conductor f of the field satisfies $f \geq 50,000$ then $h(K) > 1$. Later, in 1980, Setzer [10] examined the imaginary cyclic quartic fields K with $f < 50,000$ and determined all those wtih $h(K) = 1$. He found that

$$h(K) = 1 \Leftrightarrow f = 5, 13, 16, 29, 37, 53, 61.$$

Turning next to cyclotomic fields, Masley and Montgomery [8] in 1976 determined all cyclotomic fields $K = Q(e^{2\pi i/n})$ $(n \not\equiv 2 (\text{mod } 4))$ for which $h(K) = 1$. They proved that

$$\begin{aligned} h(K) = 1 \Leftrightarrow n = & 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, \\ & 19, 20, 21, 24, 25, 27, 28, 32, 33, 35, \\ & 36, 40, 44, 45, 48, 60, 84. \end{aligned}$$

Also in 1976 Masley [7] determined the cyclotomic fields K for which $2 \leq h(K) \leq 10$.

There are also results for other types of fields. I just mention that Uchida [13] has determined all those imaginary octic fields $Q(\sqrt{d_1}, \sqrt{d_2}, \sqrt{d_3})$ with classnumber 1. He showed that there are just 17 such fields.

The determination of all imaginary cyclic quartic fields of classnumber 2 does not appear to have been dealt with in the literature. In this talk I will describe briefly the solution to the classnumber 2 problem for these fields.

2. Cyclic quartic extensions of Q. It is shown in [6] that every cyclic quartic extension K of Q can be written in the form

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

where

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

Moreover any field of the form (2.1) satisfying (2.2) is a cyclic quartic extension of Q. Further, the representation (2.1), (2.2) is unique in the sense that if $K = Q(\sqrt{A_1(D_1 + B_1\sqrt{D_1})})$ is another representation of K satisfying (2.2) then $A = A_1, B = B_1, C = C_1, D = D_1$.

In [6] the discriminant $d(K)$ of the field K is determined in terms of A, B, C, D. It is shown that

$$d(K) = 2^e A^2 D^3, \tag{2.3}$$

where

$$e = \begin{cases} 8, & \text{if } D \equiv 2 (\text{mod } 8)\ , \\ 6, & \text{if } D \equiv 1 (\text{mod } 4), B \equiv 1 (\text{mod } 2)\ , \\ 4, & \text{if } D \equiv 1 (\text{mod } 4), B \equiv 0 (\text{mod } 2), A + B \equiv 3 (\text{mod } 4)\ , \\ 0 & \text{if } D \equiv 1 (\text{mod } 4), B \equiv 0 (\text{mod } 2), A + B \equiv 1 (\text{mod } 4)\ . \end{cases} \tag{2.4}$$

By the discriminant-conductor formula we have

$$d(K) = mf^2, \tag{2.5}$$

where m is the conductor of $k = Q(\sqrt{D})$ the unique (real) quadratic subfield of K. As

$$m = \begin{cases} D, & \text{if } D \equiv 1 (\text{mod } 4), \\ 4D, & \text{if } D \equiv 2 (\text{mod } 8), \end{cases} \tag{2.6}$$

we have

$$f = 2^{\ell} |A| D, \tag{2.7}$$

where

$$\ell = \begin{cases} 3, & \text{if } D \equiv 2 (\text{mod } 8) \text{ or } D \equiv 1 (\text{mod } 4), B \equiv 1 (\text{mod } 2), \\ 2, & \text{if } D \equiv 1 (\text{mod } 4), B \equiv 0 (\text{mod } 2), A + B \equiv 3 (\text{mod } 4), \\ 0, & \text{if } D \equiv 1 (\text{mod } 4), B \equiv 0 (\text{mod } 2), A + B \equiv 1 (\text{mod } 4). \end{cases} \tag{2.8}$$

3. Formulae for $h(K)$. Let G denote the multiplicative group of residues coprime with f so that G is isomorphic in a natural way to $Gal(Q(e^{2\pi i/f})/Q)$. We let H denote the subgroup of G, which is isomorphic to $Gal(Q(e^{2\pi i/f})/K)$. By galois theory we know that G/H is a cyclic group of order 4, say

$$G/H = < \alpha\, H > \tag{3.1}$$

In what we do the particular choice of α will not be important. We define a character χ on G by

$$\chi(\alpha) = i,\ \chi(h) = 1\ \forall\ h \in H. \tag{3.2}$$

It is easy to show that all the characters on G, which are trivial on H, are given by

$$\chi_0,\ \chi,\ \chi^2,\ \chi^3, \tag{3.3}$$

where $\chi^4 = \chi_0$ is the trivial character on G. The characters χ and $\chi^3 = \overline{\chi}$ are both odd primitive characters of conductor f. The character χ^2 however may not be primitive. The primitive character $(\chi^2)'$ induced by χ^2 is

$$(\chi^2)'(n) = \left(\frac{m}{n}\right), n > 0, (n, m) = 1, \tag{3.4}$$

where m is the conductor of $k = Q(\sqrt{D})$.

For s a complex variable, we set

$$L_1(s) \;=\; L(s,\chi)\, L(s,\chi^3) \tag{3.5}$$

and

$$L_2(s) = L(s,\chi^2). \tag{3.6}$$

It follows from [6] that

$$\frac{h(K)}{h(k)} = \frac{f w(K) L_1(1)}{4\pi^2},$$

where $w(K)$ denotes the number of roots of unity in K, that is,

$$w(K) = \begin{cases} 2, & \text{if } f > 5, \\ 10, & \text{if } f = 5. \end{cases} \tag{3.7}$$

Since $h(K) = 1$ when $f = 5$, we may assume that $f > 5$. As k is the maximal real subfield of K, the classnumber $h(k)$ divides the classnumber $h(K)$, and the integer $h(K)/h(k)$ is called the relative classnumber of K (over k) and is denoted by $h^*(K)$. Thus we have

$$h^*(K) = \frac{f L_1(1)}{2\pi^2}, \; f > 5. \tag{3.8}$$

From the work of Berndt [2], we know that

$$L(1,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n} = \frac{\pi \sum_{0<n<f/2} \bar{\chi}(n)}{iG(\bar{\chi})\,(\chi(2)-2)}, \tag{3.9}$$

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

$$G(\chi) = \sum_{j=1}^{f} \chi(j)\, e^{2\pi i j/f}. \tag{3.10}$$

Since

$$G(\chi)\, G(\overline{\chi}) = -f, \tag{3.11}$$

we obtain

$$L_1(1) = \frac{\pi^2}{f(\chi(2)-2)(\overline{\chi}(2)-2)} \left| \sum_{0<n<f/2} \chi(n) \right|^2 \tag{3.12}$$

and so

$$h^*(K) = \rho \left| \sum_{0<n<f/2} \chi(n) \right|^2, \; f > 5, \tag{3.13}$$

where

$$\rho = \begin{cases} \frac{1}{8}, & f \text{ even}, \\ \frac{1}{2}, & f \text{ odd}, \chi(2) = 1, \\ \frac{1}{18}, & f \text{ odd}, \chi(2) = -1, \\ \frac{1}{10}, & f \text{ odd}, \chi(2) = \pm i. \end{cases} \tag{3.14}$$

Defining, for $j = 0, 1, 2, 3,$

(3.15)
$$C_j = \sum_{\substack{0<n<f/2 \\ \chi(n)=i^j}} 1 = \sum_{\substack{0<n<f/2 \\ n\in\alpha^j H}} 1,$$

we obtain

(3.16)
$$h^*(K) = \rho\{(C_0 - C_2)^2 + (C_1 - C_3)^2\}.$$

4. Lower bound for $h^*(K)$. By extending the ideas used in [13], and the formula (3.8), it can be shown that

(4.1)
$$h^*(K) > 2 \text{ for } f \geq 416,000.$$

Thus in order to determine all imaginary cyclic quartic fields with $h^*(K) = 2$ it suffices to consider only those having $f < 416,000$.

5. Necessary and sufficient condition for $h^*(K) \equiv 2 \pmod 4$. In searching the imaginary cyclic quartic fields K of conductor $f < 416,000$ for those fields with $h^*(K) = 2$, it suffices to calculate $h^*(K)$ only for those fields K having $h^*(K) \equiv 2 (\text{mod } 4)$. It is shown in [6] that

(5.1)
$$\begin{aligned} h^*(K) \equiv 2 (\text{mod } 4) & \\ & \Leftrightarrow f = 16p, \text{ where } p \equiv 3 \text{ or } 5 \pmod 8, \\ & \text{or } f = 8p, \text{ where } p \equiv 5 (\text{mod } 8), \\ & \text{or } f = pq, \text{ where } (p/q) = -1. \end{aligned}$$

Here p and q denote distinct odd primes. This considerably reduces the number of fields K for which $h^*(K)$ must be calculated.

6. Calculation of $h^*(K)$. Using the formula for $h^*(K)$ given in (3.16) and the results of §2, $h^*(K)$ was calculated by the method described in [6] for all fields K with $f < 416,000$ and f of

the form (5.1). It was found that

$$
\begin{aligned}
h^*(K) = 2 \Leftrightarrow K = & Q(\sqrt{-(5+\sqrt{5})}) && (f = 40) \\
& Q(\sqrt{-3(2+\sqrt{2})}) && (f = 48) \\
& Q(\sqrt{-5(13+2\sqrt{13})}) && (f = 65) \\
& Q(\sqrt{-13(5+2\sqrt{5})}) && (f = 65) \\
& Q(\sqrt{-5(2+\sqrt{2})}) && (f = 80) \\
& Q(\sqrt{-(10+3\sqrt{10})}) && (f = 80) \\
& Q(\sqrt{-17(5+2\sqrt{5})}) && (f = 85) \\
& Q(\sqrt{-(85+6\sqrt{85})}) && (f = 85) \\
& Q(\sqrt{-(13+3\sqrt{13})}) && (f = 104) \\
& Q(\sqrt{-7(17+4\sqrt{17})}) && (f = 119)
\end{aligned}
$$

7. Solution of classnumber 2 problem. We have

$$h(K) = 2 \Leftrightarrow h^*(K) = 2, h(k) = 1$$

or

$$h^*(K) = 1, h(k) = 2.$$

However from [10] we know that

$$h^*(K) = 1, h(k) = 2$$

cannot occur so that

$$h(K) = 2 \Leftrightarrow h^*(K) = 2, h(k) = 1.$$

Thus $h(K) = 2$ occurs only for those fields K in the list of §6 for which $h(k) = 1$. Since

$$h\left(Q(\sqrt{2})\right) = h\left(Q(\sqrt{5})\right) = h\left(Q(\sqrt{13})\right) = h\left(Q(\sqrt{17})\right) = 1$$

and

$$h\left(Q(\sqrt{10})\right) = h\left(Q(\sqrt{85})\right) = 2,$$

we have proved the following theorem.

THEOREM. Let K be an imaginary cyclic quartic field. Then $h(K)=2$ if and only if

$$K = Q\left(\sqrt{-3(2+\sqrt{2})}\right), Q\left(\sqrt{-5(2+\sqrt{2})}\right), Q\left(\sqrt{-(5+\sqrt{5})}\right),$$
$$Q\left(\sqrt{-13(5+2\sqrt{5})}\right), Q\left(\sqrt{-17(5+2\sqrt{5})}\right), Q\left(\sqrt{-(13+3\sqrt{13})}\right),$$
$$Q\left(\sqrt{-5(13+2\sqrt{13})}\right), \quad \text{or} \quad Q\left(\sqrt{-7(17+4\sqrt{17})}\right).$$

REFERENCES

1. A. Baker, Imaginary quadratic fields with class number 2, Annals of Math. 94 (1971), 139-152.

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

3. E. Brown and C.J. Parry, The imaginary bicyclic biquadratic fields with class number 1, J. für reine angew. Math. 266 (1974), 118-120.

4. D.A. Buell, H.C. Williams and K.S. Williams, On the imaginary bicyclic biquadratic fields with class-number 2, Math. Comp. 31 (1977), 1034-1042.

5. L. Carlitz, A characterization of algebraic number fields with class number two, Proc. Amer. Math. Soc. 11 (1960), 391-392.

6. 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 Note Series No. 7, July 1986, 201 pp.

7. J.M. Masley, Solution of small class number problems for cyclotomic fields, Compositio Mathematica 33(1976), 179-186.

8. J.M. Masley and H.L. Montegomery, Cyclotomic fields with unique factorization, J. für reine angew. Math. 286/287 (1976), 248-256.

9. J.-F. Mestre, Courbes de Weil et courbes supersingulières, Séminaire de Théorie des Nombres de Bordeaux, Année 1984-1985, exposé 23, 1-6.

10. B. Setzer, The determination of all imaginary, quartic, abelian number fields with class number 1, Math. Comp. 35 (1980), 1381-1386.

11. H.M. Stark, A complete determination of the complex quadratic fields of class-number one, Mich. Math. J. 14 (1967), 1-27.

12. H.M. Stark, On complex quadratic fields with class-number two, Math. Comp. 29(1975), 289-302.

13. K. Uchida, Imaginary abelian number fields with class number one, Tôhoku Math. J. 24(1972), 487-499.