MATHEMATICS OF COMPUTATION, VOLUME 31, NUMBER 140
OCTOBER 1977, PAGES 1019–1029

Real Quadratic Fields With Class Numbers Divisible by Five

By Charles J. Parry

Abstract. Conditions are given for a real quadratic field to have class number divisible by five. If 5 does not divide m, then a necessary condition for 5 to divide the class number of the real quadratic field with conductor m or $5m$ is that 5 divide the class number of a certain cyclic biquadratic field with conductor $5m$. Conversely, if 5 divides the class number of the cyclic field, then either one of the quadratic fields has class number divisible by 5 or one of their fundamental units satisfies a certain congruence condition modulo 25.

1. Introduction. While a necessary and sufficient condition for 3 to divide the class number of a real quadratic field has been given by Herz [3], no similar condition seems to exist for 5. In this article, we will extend the methods of Herz to obtain such a result. Although Weinberger [9] and Yamatoto [10] have proved the existence of infinitely many real quadratic fields with class number divisible by any integer n, their results are quite different from those of Herz and those of this article.

Certainly 5 divides the class number of one of the quadratic fields $k_1 = Q(\sqrt{m})$ or $k_2 = Q(\sqrt{5m})$ if and only if 5 divides the class number of their biquadratic compositum K_1. We show if 5 divides the class number of K_1 then 5 divides the class number of a certain imaginary cyclic biquadratic field K_2 with conductor $5D$, where D is the discriminant of k_1. Conversely, if 5 divides the class number of K_2, then either 5 divides the class number of K_1 or one of three congruence conditions holds modulo 5 or 25 on the fundamental units of k_1 or k_2.

2. Notation.

$\zeta = e^{2\pi i/5}$.

m: a square free positive rational integer with $(5, m) = 1$.

Q: the field of rational numbers.

$k_1 = Q(\sqrt{m})$.

$k_2 = Q(\sqrt{5m})$.

$k_3 = Q(\sqrt{5})$.

$L = Q(\zeta, \sqrt{m})$.

$K_1 = Q(\sqrt{5}, \sqrt{m})$.

$K_2 = Q(\sqrt{-10m + 2m\sqrt{5}})$: cyclic biquadratic subfield of L.

$K_3 = Q(\zeta)$.

D = discriminant of the field k_1.

h = class number of L.

Received August 5, 1976; revised December 16, 1976.
AMS (MOS) subject classifications (1970). Primary 12A25; Secondary 12A50.

h_i ($i = 1, 2, 3$): class number of K_i.
h_i^* ($i = 1, 2, 3$): class number of k_i.
$\hat{E}$: the group of units of L.
$\hat{e}$: the subgroup of $\hat{E}$ generated by the units of fields K_i ($i = 1, 2, 3$).
$\hat{\epsilon}$: the subgroup of $\hat{e}$ generated by the units of the fields k_i ($i = 1, 2, 3$).
$Q_0 = (\hat{E} : \hat{e})$.
$Q_1 = (\hat{e} : \hat{\epsilon})$.
ϵ_i ($i = 1, 2, 3$): the fundamental unit of the field k_i.

3. Class Number Relations.

THEOREM 1. $2h = h_1 h_2$.

Proof. Since the Galois group of L/k_3 is bicyclic of order 4, it follows from Theorem 5.5.1 of Walter [8] that $2hh_3^* = Q_0 h_1 h_2 h_3$. However, it is well known that $h_3 = h_3^* = 1$.

To complete the proof we need to show $Q_0 = 1$. If $E \in \hat{E}$, Theorem 1 of Parry [7] shows

$$E^2 = \pm \zeta e = \pm \zeta^6 e,$$

where $e \in K_1$. Thus,

$$(E/\zeta^3)^2 = \pm e.$$

If $e_1 = E/\zeta^3 \notin K_1$, then $L = K_1(e_1) = K_1(\sqrt{\pm e})$ so only the prime divisors of 2 in K_1 could ramify in L. However, the prime divisors of 5 in K_1 ramify in L. Thus, $e_1 \in K_1$ and so $E = \zeta^3 e_1 \in \hat{e}$. Hence, $\hat{E} \subset \hat{e}$ so $Q_0 = 1$.

THEOREM 2. $4h_1 = Q_1 h_1^* h_2^*$ *with* $Q_1 = 1$ *or* 2.

Proof. Immediate from Satz 1 of Kubota [5] and Satz 11 of Kuroda [6] since $h_3^* = 1$ and the fundamental unit of k_3 has norm -1.

COROLLARY 3. $8h = Q_1 h_1^* h_2^* h_2$.

4. Class Number Divisibility.

LEMMA 4. *If* $5 \mid h_1$, *then* $5 \mid h_2$.

Proof. If M/K_1 is cyclic of degree 5, then $M(\zeta)/K_1$ is cyclic of degree 10. A generator σ of the Galois group $G(M/K_1)$ can be extended to an element of $G(M(\zeta)/K_1)$ by setting $\zeta^\sigma = \zeta$. Hilbert's Theorem 90 gives an element $\alpha \in M(\zeta)$ satisfying $\alpha^{\sigma - 1} = \zeta$. Moreover, α is uniquely determined up to multiplication by $\beta \in L$.

Let ρ be the unique element of $G(M(\zeta)/K_1)$ which has order 2 and define quantities θ, a and e by $\theta = \alpha + \alpha^\rho$, $a = \alpha^{1+\rho}$ and $e = \alpha^{4-\rho} + \alpha^{4\rho - 1}$. Now $a, e \in K_1$, $\theta \in M$, $M = K_1(\theta)$ and $\theta^5 - 5a\theta^3 + 5a^2\theta - ae = 0$. Since M/k_3 is dihedral, the nontrivial automorphism of K_1/k_3 can be extended to an automorphism τ of $M(\zeta)/k_3$ satisfying the following properties:

$$\zeta^\tau = \zeta^4, \quad \tau^2 = 1, \quad \rho\tau = \tau\rho, \quad \tau\sigma = \sigma^4\tau.$$

If $\beta = \alpha^{\tau - 1}$ then

$$\beta^\sigma = (\alpha^{\tau-1})^\sigma = \alpha^{\sigma^4\tau - \sigma} = (\zeta^4\alpha)^\tau/(\zeta\alpha) = \zeta\alpha^\tau/\zeta a = \alpha^{\tau-1} = \beta,$$

so that $\beta \in L$. Replace α with $(1 + \beta)\alpha$ if $\beta \neq -1$ and with $(\zeta - \zeta^4)\,\alpha$ if $\beta = -1$. This gives $\alpha = \alpha^\tau$ so that $\alpha^5 \in K_2$ and α is uniquely determined up to a factor γ of K_2. Thus we can take α to be an integer of K_2 and so a and e will be integers of k_3. Theorem 1 of Parry [7] shows that the only units of K_2 are the units of k_3, so if α^5 were a unit of K_2, then $\alpha^5 \in K_1$. This would mean that $M = K_1(\alpha) = K_1(\sqrt[5]{\alpha^5})$ and so M/K_1 would be a nonnormal extension. Thus, α^5 is not a unit of K_2.

If $5 \mid h_1$, then we may assume M/K_1 is unramified; and hence, $M(\zeta)/L$ is also unramified. Because $M(\zeta) = L(\sqrt[5]{\alpha^5})$, a prime ideal $\mathfrak{P}$ of L can divide (α^5) if and only if $\mathfrak{P}^5$ divides (α^5). Since $\alpha^5 \in K_2$, a prime ideal $\mathfrak{p}$ of K_2 will divide (α^5) if and only if $\mathfrak{p}^5$ divides (α^5). Since we may assume α^5 is not divisible by a fifth power of another integer of K_2 (except units), it follows $(\alpha^5) = (\mathfrak{p}_1 \cdots \mathfrak{p}_t)^5$ where $\mathfrak{p}_1 \cdots \mathfrak{p}_t$ is a nonprincipal ideal of K_2 whose fifth power is principal. Thus, 5 divides h_2.

THEOREM 5 (MAIN RESULT). *If $5 \mid h_2$, then either $5 \mid h_1$ or the fundamental units $\epsilon_1 = (a + b\sqrt{m})/2$ of k_1 and $\epsilon_2 = (c + d\sqrt{5m})/2$ of k_2 satisfy one of the following conditions*:

(1) $a \equiv 0$ *or* $b \equiv 0 \pmod{25}$.

(2) $m \equiv \pm 2 \pmod 5$ *and* $\epsilon_1 \equiv \pm\epsilon$ *or* $\pm 7\epsilon \pmod{25}$ *where* $\epsilon = r \pm m^2\sqrt{m}$ *with* $r = 9$ *or* 12 *according as* $m \equiv 2$ *or* $-2 \pmod 5$.

(3) $d \equiv 0 \pmod 5$.

Conversely, if $5 \mid h_1$ or one of conditions (1)–(3) *holds, then* $5 \mid h_2$.

Proof. We begin by reversing the roles of K_1 and K_2 in the proof of the preceding lemma. Thus, if $5 \mid h_2$, then M/K_2 is an abelian unramified extension of degree 5 and $M(\zeta) = L(\alpha)$ with $\alpha^5 \in K_1$. If α^5 is not a unit of K_1, then it follows as in Lemma 4 that $5 \mid h_1$. If $\alpha^5 = e$ is a unit of K_1, then α may be replaced with α^2 so that $\alpha^5 = e = e_1e_2e_3$ with $e_i \in k_i$ $(i = 1, 2, 3)$ (see Theorems 1 and 2). Satz 119 of Hecke [2] shows that $L(\sqrt[5]{e})/L$; and hence, M/K_2 will be an unramified extension if and only if

$$(4) \qquad x^5 \equiv e \mod (1 - \zeta)^5$$

is solvable in L. By applying the relative norm function for L/K_1, it is seen that (4) is solvable if and only if

$$(5) \qquad x^5 \equiv e \mod (5\sqrt{5})$$

is solvable in K_1. Applying the relative norm functions for K_1/k_i $(i = 1, 2, 3)$ to (5) shows that

$$(6) \qquad x^5 \equiv e_1 \mod (25),$$

$$(7) \qquad x^5 \equiv e_2 \mod \mathfrak{p}_5^3,$$

$$(8) \qquad x^5 \equiv e_3 \mod (5\sqrt{5})$$

(where $\mathfrak{p}_5 = (5, \sqrt{5m})$) must be solvable in k_1, k_2 and k_3, respectively. First of all, it is easy to see that (8) has no solution unless e_3 is the fifth power of a unit of k_3. Thus, we may take $e_3 = 1$ and $\alpha^5 = e = e_1e_2$. Next observe (7) is solvable if and only if $e_2 \equiv u + v\sqrt{5m} \pmod 5$ with $v \equiv 0 \pmod 5$. Suppose $e_2 = \epsilon_2^t$ where ϵ_2 is the fundamental unit of k_2. Certainly, we may assume that t is reduced modulo 5. Moreover, if $t \not\equiv 0 \pmod 5$, then (7) has a solution if and only if

$$x^5 \equiv \epsilon_2 \mod \mathfrak{p}_5^3$$

has a solution; i.e. we may assume $t = 0$ or 1. If $t = 1$, then condition (3) of the theorem holds. If $t = 0$, then $e_1 \neq \pm 1$, since otherwise α would be a 10th root of unity. Hence, we may assume that (6) holds where $e_1 = \epsilon_1$ is the fundamental unit of k_1.

We need to determine exactly when

$$x^5 \equiv \epsilon_1 \pmod{25} \tag{9}$$

has a solution in k_1.

If $m \equiv \pm 1 \pmod 5$, then $(25) = (\mathfrak{p}_1 \mathfrak{p}_2)^2$ in k_1 where $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are distinct prime ideals. Now (9) has a solution if and only if

$$x^5 \equiv \epsilon_1 \pmod{\mathfrak{p}_i^2} \tag{10}$$

has a solution for $i = 1, 2$. Also, the reduced residue system modulo 25 forms a reduced residue system modulo $\mathfrak{p}_i^2$; and the fifth powers modulo $\mathfrak{p}_i^2$ are precisely ± 1 and ± 7. If $\epsilon_1 \equiv u + v\sqrt{m} \pmod{25}$, then $\pm 1 \equiv u^2 - mv^2 \pmod{25}$; and since $m \equiv \pm 1 \pmod 5$, either $u \equiv 0$ or $v \equiv 0 \pmod 5$. It follows that $u^2 \equiv \pm 1$ or $mv^2 \equiv \pm 1 \pmod{25}$, and thus $u \equiv \pm 1, \pm 7$ or $\sqrt{m}v \equiv \pm 1, \pm 7 \pmod{\mathfrak{p}_i^2}$. Suppose

$$\epsilon_1 \equiv u + v\sqrt{m} \pmod{\mathfrak{p}_i^2},$$

where $v \equiv 0 \pmod 5$. Thus, both ϵ_1 and u are fifth power residues and $v \equiv 0 \pmod{\mathfrak{p}_i}$. It follows that

$$\epsilon_1 \equiv u \pmod{\mathfrak{p}_i^2},$$

and so $v\sqrt{m} \equiv 0 \mod \mathfrak{p}_i^2$ which implies $v \equiv 0 \pmod{25}$. A similar argument shows that $u \equiv 0 \pmod{25}$ when $u \equiv 0 \pmod 5$.

If $m \equiv \pm 2 \pmod 5$, then 5 stays prime in k_1; and there are 600 reduced residues modulo 25, 24 of which are fifth powers. A complete set of fifth power residues may be obtained by taking all products from the sets

$$S = \{\pm 1, \pm 7, \pm m^2\sqrt{m}, \pm 7m^2\sqrt{m}\} \quad \text{and} \quad T = \{\pm 1, r \pm m^2\sqrt{m}\},$$

where $r = 9$ or 12 according as $m \equiv 2$ or $m \equiv 3 \pmod 5$. Note that $r^2 - m^5 \equiv 1$ or $-1 \pmod{25}$ according as $m \equiv 3$ or $m \equiv 2 \pmod 5$. Thus, only ± 1 and ± 7 times $r \pm m^2\sqrt{m}$ can be units. It is now obvious that (9) has a solution if and only if (1) or (2) holds.

We have now proved that if $5 \mid h_2$ and $5 \nmid h_1$, then one of (1)–(3) must hold. Conversely, if one of (1)–(3) holds, set $e = \epsilon_1$ if (1) or (2) holds and $e = \epsilon_2$ if (3) holds. The above discussion shows that (4) has a solution for this choice of e. Satz 119 of Hecke [2] shows that $L(\sqrt[5]{e})/L$ is unramified so that $5 \mid h$. Theorem 1 shows $5 \mid h_1$ or $5 \mid h_2$. If $5 \mid h_1$, then Lemma 4 shows $5 \mid h_2$, also.

The following corollary gives a more convenient version of condition (2).

COROLLARY 6. *The fundamental unit* ϵ_1 *of* k_1 *satisfies condition* (2) *if and only if* $\mathrm{Tr}(\epsilon_1) \equiv \pm 1, \pm 7 \pmod{25}$ *where* Tr *denotes the trace function.*

Proof. Certainly, if ϵ_1 satisfies condition (2), then $\mathrm{Tr}(\epsilon_1) \equiv \pm 1, \pm 7 \pmod{25}$. Conversely, suppose $\epsilon = \epsilon_1 \equiv a + b\sqrt{m} \pmod{25}$ with $\mathrm{Tr}(\epsilon) \equiv 2a \equiv \pm 1, \pm 7 \pmod{25}$. Thus,

$$\pm 1 \equiv N(\epsilon) \equiv a^2 - b^2 m \pmod{25},$$

so

$$\pm 4 \equiv 4a^2 - 4b^2 m \equiv \mathrm{Tr}(\epsilon)^2 - 4b^2 m$$

$$\equiv \pm 1 - 4b^2 m \pmod{25}.$$

Since $m \not\equiv 0 \pmod 5$, the choice of $\pm$ signs must be the same on both sides and, in fact, is the sign of $\mathrm{Tr}(\epsilon)^2$. Thus,

$$4b^2 m \equiv -3\ \mathrm{Tr}(\epsilon)^2 \pmod{25},$$

so

$$b^2 m \equiv 18\ \mathrm{Tr}(\epsilon)^2 \equiv -7\ \mathrm{Tr}(\epsilon)^2 \pmod{25}.$$

Squaring gives

$$b^4 m^2 \equiv -1 \pmod{25},$$

so

$$b \equiv -b^5 m^2 \pmod{25}.$$

Now

$$b^2 m \equiv -7\ \mathrm{Tr}(\epsilon)^2 \equiv -2\ \mathrm{Tr}(\epsilon)^2 \pmod 5,$$

so

$$b^2 \equiv \pm \mathrm{Tr}(\epsilon)^2 \pmod 5,$$

where the sign is + if $m \equiv 3 \pmod 5$ and − if $m \equiv 2 \pmod 5$. If $m \equiv 3 \pmod 5$, then

$$b \equiv \pm \mathrm{Tr}(\epsilon) \pmod 5,$$

so

$$b \equiv -b^5 m^2 \equiv \pm \mathrm{Tr}(\epsilon) m^2 \pmod{25}.$$

Thus,

$$\epsilon \equiv a \pm \mathrm{Tr}(\epsilon) m^2 \sqrt{m} \pmod{25}$$

$$\equiv -\mathrm{Tr}(\epsilon)(12 \pm m^2\sqrt{m}) \pmod{25}.$$

If $m \equiv 2 \pmod 5$, then

$$b^2 \equiv -\mathrm{Tr}(\epsilon)^2 \pmod 5,$$

so

$$b \equiv \pm 7\ \mathrm{Tr}(\epsilon) \pmod 5.$$

Hence,

$$b \equiv -b^5 m^2 \equiv \pm 7\ \mathrm{Tr}(\epsilon) m^2 \pmod{25},$$

so

$$\begin{aligned} \epsilon &\equiv 13\ \mathrm{Tr}(\epsilon) \pm 7\ \mathrm{Tr}(\epsilon) m^2\sqrt{m} \pmod{25} \\ &\equiv -\mathrm{Tr}(\epsilon)(12 \pm 7m^2\sqrt{m}) \pmod{25} \\ &\equiv \pm 7\ \mathrm{Tr}(\epsilon)(9 \pm m^2\sqrt{m}) \pmod{25}. \end{aligned}$$

Thus, in either case (2) is satisfied.

The distinction between conditions (1) and (2) of Theorem 5 is somewhat artificial as is seen by the following result.

COROLLARY 7. *If* ϵ_1 *satisfies condition* (2), *then* ϵ_1^3 *satisfies condition* (1).

Proof. Simply cube $\epsilon = r \pm m^2\sqrt{m}$ and note that $m^5 \equiv 7$ or -7 and $r \equiv 9$ or 12 (mod 25) according as $m \equiv 2$ or $-2 \pmod 5$.

We now classify those fields K_2 which have class number divisible by 5 into three types:

Type 1. Condition (1) or (2) of Theorem 5 is satisfied.

Type 2. Condition (3) of Theorem 5 is satisfied.

Type 3. 5 divides h_1.

Type 3 fields can be subdivided into two further types:

Type 3a. 5 divides h_1^*.

Type 3b. 5 divides h_2^*.

The next corollary gives the sought after condition for 5 to divide h_1.

COROLLARY 8. *If* $5 \mid h_2$ *and* K_2 *is not of Type* 1 *or* 2, *then* $5 \mid h_1$.

COROLLARY 9. *If* K_2 *is both Type* 1 *and Type* 2, *then* $25 \mid h_2$ *and the* 5*-class group of* K_2 *is noncyclic.*

Proof. Under our assumptions $L(\sqrt[5]{\epsilon_1})$ and $L(\sqrt[5]{\epsilon_2})$ are distinct unramified abelian extensions of L of degree 5. There exist corresponding unramified abelian extensions M_1/K_2 and M_2/K_2 of degree 5 with $M_i \subset L(\sqrt[5]{\epsilon_2})$ for $i = 1, 2$. Since $L(\sqrt[5]{\epsilon_1}) \neq L(\sqrt[5]{\epsilon_2})$ we see $M_1 \neq M_2$. Thus, $M_0 = M_1M_2$ is an unramified abelian extension of K_2 of degree 25 with noncyclic Galois group. Thus, $25 \mid h_2$ and the 5-class group of K_2 is noncyclic.

COROLLARY 10. *If* K_2 *is of Type* 1 *and Type* 3b *or Type* 2 *and Type* 3a, *then* $25 \mid h_2$ *and the* 5*-class group of* K_2 *is noncyclic.*

Proof. If K_2 satisfies both Type 1 and Type 2 conditions, then we are done by Corollary 9. When K_2 is of Type 3a (3b), there exists a nonprincipal prime ideal $\mathfrak{p}$ of

k_1 (k_2) such that $\mathfrak{p}^5 = (r + s\sqrt{m})$ is principal. (Here we temporarily change notation to allow $m \equiv 0 \pmod 5$ when K_2 is Type 3b.) If we can choose $\alpha = r + s\sqrt{m}$ so that 5 does not ramify in $L(\sqrt[5]{\alpha})$, then we are done. This is so because $L(\sqrt[5]{\alpha})/L$ and $L(\sqrt[5]{\epsilon_i})/L$ ($i = 1$ or 2 according as K_2 is Type 3b or 3a) will be distinct unramified abelian extensions of degree 5. At this point, we can use the proof of Corollary 9.

In order to see that α can be chosen properly, it will be necessary to consider three cases:

Case 1. K_2 *Type* 2 *and Type* 3a, $m \equiv \pm 1 \pmod 5$. Here $(25) = (\mathfrak{p}_1\mathfrak{p}_2)^2$ where $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are prime ideals of k_1. There are 20 reduced residues modulo $\mathfrak{p}_i^2$ and the fifth powers are precisely $\pm 1, \pm 7$. Since ϵ_1 is not a fifth power residue, the powers ϵ_1^j ($j = 0, \ldots, 4$) form a complete set of coset representatives for the subgroup of fifth power residues in the whole group modulo $\mathfrak{p}_i^2$. Thus, $\epsilon_1^j(r + s\sqrt{m})$ is a fifth power residue modulo $\mathfrak{p}_i^2$ for some j. We need to observe that j does not depend on i. If

$$\epsilon_1^j(r + s\sqrt{m}) \equiv u + v\sqrt{m} \pmod{25},$$

then as in the proof of Theorem 5 we must have $u \equiv 0$ or $v \equiv 0 \pmod{25}$. Thus, $\alpha = \epsilon_1^j(r + s\sqrt{m})$ is a fifth power modulo 25 and Satz 119 of Hecke [2] shows $L(\sqrt[5]{\alpha})/L$ is an unramified extension.

Case 2. K_2 *Type* 2 *and Type* 3a, $m \equiv \pm 2 \pmod 5$. Here $L(\sqrt[5]{\alpha})/L$ will be unramified if α is a fifth power residue modulo 25. Since 5 remains prime in k_1, there are 600 reduced residues in k_1 modulo 25 and 24 of these are fifth power residues. If A denotes the ring of algebraic integers of k_1, then the norm function defines a surjective homomorphism

$$N\colon (A/25A)^* \longrightarrow (Z/25Z)^*.$$

The kernel of N must have order 30 and the preimage, H, of $\{\pm 1, \pm 7\}$ has order 120. Note that ϵ_1, α and the subgroup, F, of fifth power residues all belong to H. Since ϵ_1 is not in F, the powers ϵ_1^j ($j = 0, \ldots, 4$) give a complete set of coset representatives for F in H. Thus, $\epsilon_1^j\alpha \in F$ for some choice of j. If α is replaced by $\epsilon_1^j\alpha$, then $L(\sqrt[5]{\alpha})/L$ will be unramified.

Case 3. K_2 *Type* 1 *and Type* 3b, $m \equiv 0 \pmod 5$. We shall now return to our standard notation and write $\alpha = r + s\sqrt{5m}$ with $(m, 5) = 1$. Now $L(\sqrt[5]{\alpha})/L$ will be unramified if and only if α is a fifth power residue modulo $\mathfrak{p}_5^3$ where $\mathfrak{p}_5 = (5, \sqrt{5m})$. There are 100 reduced residues modulo $\mathfrak{p}_5^3$, and the subgroup of fifth power residues is $F = \{\pm 1, \pm 7\}$. If A denotes the ring of algebraic integers of k_2, then the norm function defines a homomorphism

$$N\colon (A/\mathfrak{p}_5^3)^* \longrightarrow (Z/25Z)^*.$$

Since only integers congruent to $\pm 1 \pmod 5$ can be norms, the image of N has order 10. The kernel of N must also have order 10 and the preimage, H, of $\langle \pm 1 \rangle$ has order 20. Note that ϵ_2, α and F all belong to H. Since $\epsilon_2 \notin F$ we have, as in Case 2, $\epsilon_2^j\alpha \in F$ for some j. This completes the proof.

TABLE I $(m = p)$

D	h_2	h_2^*	type
37	10		2
53	10		1
73	10		1
89	20		1
92	20		2
109	20		1
124	40		2
149	20		2
236	80		2
241	40		1
257	50		1,2
281	40		2
293	50		2
313	50		2
401	80		3a
428	100		1
433	90		1
457	50	2	1,2
508	100		1,2
509	100	4	1,2
541	80		1
556	80		1
557	130	2	2
617	130		1
673	90		1
761	80	4	1
764	200		1,2
796	160		2
809	100	4	2
844	200		1
857	170		1
881	200	2	1,2
892	260		2
908	180		2
937	130	2	2
997	130	2	2
1069	100	2	2
1084	200		1
1093	250	2	3a
1097	170	2	2
1129	180	2	2
1193	290	2	2
1213	250	2	1
1217	170	10	3b
1228	260		2
1289	180		1
1301	200	2	1
1321	360		1
1388	180		2
1428	180		2
1429	180	2	3a
1493	250	18	1,2
1597	250	2	1,2
1621	320		1
1637	450	14	1
1721	400	4	2
1741	400	4	1
1756	320	2	3a
1777	370		1
1861	320		1
1868	500	10	1,3b
1913	250	2	1,2
1916	320	2	2
1949	260	6	2
1973	370	2	2
1996	400	6	2,3a
2092	340	2	1
2348	500	2	1,2
2524	520	2	2
2572	500	2	2
2732	740	2	2
2876	640		1
2908	740	2	3a
2972	580	2	2
3356	1280	2	2
3548	740	2	2
3644	1000	10	3b
3788	900	2	1
3932	1220		1
4124	680		1
4204	680		1
4252	820	2	2
4348	1220		1
4492	1780	10	2,3b
4748	900	2	1
4924	1000	2	1,2
5116	1600	10	1,3b
5164	1960	2	2
5308	900	2	2,3a
5708	1220	2	1
5804	1000	2	2
5932	1220	6	2
6044	1640	2	2
6124	1000	6	1,2
6284	1640	2	2
6316	1360	2	2
6652	1940		1
6796	2320		1
6892	1780		1
7132	2340	2	2
7388	1300	10	3b
7628	1700	2	1,2
7916	1360	10	3b
7996	1600	6	1,2
8012	2900	2	1,2

TABLE II ($m = 2p$)

m	h_2	h_2^*	type
14	20		2
26	20		2
38	40		1
62	40		1
82	80		1
86	100		2
134	100		1
202	200		1
214	260		1
278	360		1
298	400		1,2
314	260		1
326	260		1
358	200		2
382	360		1
398	320		2
422	400	2	1
446	340	6	2
458	320	4	2
466	580	4	1
502	400	6	1,2
514	340		1
526	500	2	1,2
554	740	4	2
622	520		1
626	500	4	1,2
634	340		1
662	400	2	1
674	580		1
734	500	6	1,2
758	520	2	2
766	500	2	2
794	740	20	3b
842	520	4	2
922	1000	4	1,2
926	740	2	2
982	1040	6	1,3a
1006	1220	2	2
1018	640	4	2
1042	800	8	1
1114	1460	4	2
1126	900	10	2,3a,3b
1142	1360	2	2
1198	800	2	2
1214	1220		1
1226	1460	4	3a
1238	1000	2	1,2
1262	1160		1
1294	1300	2	2
1354	1220	12	2
1366	900	2	1,2
1382	1040		1
1402	1960		1
1466	1620	20	3b
1478	1640	2	2
1486	1460	2	3a
1514	900	20	3b
1546	820	4	2
1654	1300	2	2
1658	1040		1
1754	2340		1
1762	1360		1
1766	1700	2	3a
1838	2080		1
1874	2340		1
1882	1960	20	3b
1934	1700	10	3b
1954	1460	4	2
1966	1300	6	1
1982	1160		1

It is interesting to note that when $m = 982$, K_2 is of Types 1 and 3a and when $m = 1123$, K_2 is of Types 2 and 3b. However, 25 does *not* divide h_2 in either case!

COROLLARY 11. *If K_2 is of both Type* 3a *and Type* 3b, *then* $25 \mid h_2$ *and the 5-class group of K_2 is noncyclic.*

Proof. Corollary 10 shows that we may assume that K_2 is of neither Type 1 nor Type 2. Thus, as in the proof of that corollary, we may choose $\alpha_i \in k_i$ such that $L(\sqrt[5]{\alpha_i})/L$ $(i = 1, 2)$ is an unramified abelian extension of degree 5. Moreover, we may assume $(\alpha_i) = \mathfrak{p}_i^5$ where $\mathfrak{p}_i$ is a nonprincipal prime ideal of k_i ($i = 1, 2$). If $L(\sqrt[5]{\alpha_1}) = L(\sqrt[5]{\alpha_2})$, then $\alpha_1 = \beta^5\alpha_2^t$ for some $\beta \in K_1$ and $t = 1, 2, 3$ or 4. Applying the norm function for K_1/k_1 gives $\alpha_1^2 = (N(\beta)p_2^t)^5$, where p_2 is a prime integer. Since $L(\sqrt[5]{\alpha_1})/L$ is of degree 5, we must have $L(\sqrt[5]{\alpha_1}) \neq L(\sqrt[5]{\alpha_2})$. The proof of Corollary 9 now applies.

COROLLARY 12. *Let K_2 be of Type i ($i = 1$ or 2), $\epsilon = \epsilon_i$ and $\theta = \sqrt[5]{\epsilon} + \sqrt[5]{\epsilon'}$, where ϵ' denotes the conjugate of ϵ and both fifth roots are real. Then $M = K_2(\theta)$ is an unramified abelian extension of K_2 of degree 5 and θ is a root of*

$$f(x) = x^5 - 5N(\epsilon)x^3 + 5x - \mathrm{Tr}(\epsilon),$$

where $N(\epsilon)$ and $\mathrm{Tr}(\epsilon)$ *denote the norm and trace of ϵ.*

Proof. Merely reverse the roles of K_1 and K_2 in the proof of Lemma 4. Under our assumptions we can take $\alpha = \sqrt[5]{\epsilon}$ and $\alpha^\rho = \sqrt[5]{\epsilon'}$. It is easy to see $a = N(\epsilon)$ and $ae = \mathrm{Tr}(\epsilon)$.

5. Numerical Results. Since K_2 is an imaginary cyclic biquadratic field, its class number can be readily computed using a result of Hasse [1]. The formula is

$$h_2 = \frac{1}{2\mathfrak{f}^2}\left|\sum_{n \pmod{\mathfrak{f}}} \chi(n)n\right|^2,$$

where $\mathfrak{f}$ is the conductor of K_2, the summation is over the smallest reduced residue system modulo $\mathfrak{f}$ and $\chi(n) = (m/n)\chi_1(n)$. Here (m/n) is the Jacobi symbol and $\chi_1(n)$ is a primitive character modulo 5 defined by $\chi_1(2) = i = \sqrt{-1}$. The conductor $\mathfrak{f} = 5D$ where D is the discriminant of k_1. When $\mathfrak{f}$ is even, we can make the following simplification:

THEOREM 13. *If $\mathfrak{f}$ is even, then*

$$h_2 = \frac{1}{8}\left|\sum_{n \pmod{\mathfrak{f}/2}} \chi(n)\right|^2.$$

Proof. Note that

$$\chi(n + \mathfrak{f}/2) = \left(\frac{m}{n + \mathfrak{f}/2}\right)\chi_1(n + \mathfrak{f}/2) = \left(\frac{m}{n + \mathfrak{f}/2}\right)\chi_1(n),$$

since $\mathfrak{f}/2 = 10m$. Now either m is odd or $m = 2r$ with r odd. In the first case $m \equiv 3 \pmod 4$ and in both cases n is odd. In the former case

$$\begin{aligned}\left(\frac{m}{10m + n}\right) &= (-1)^{((m-1)/2)(10m+n-1)/2}\left(\frac{10m + n}{m}\right)\\ &= (-1)^{(n+1)/2}\left(\frac{n}{m}\right) = (-1)^{(n+1)/2}(-1)^{(n-1)/2}\left(\frac{m}{n}\right)\\ &= -\left(\frac{m}{n}\right).\end{aligned}$$

In the second case

$$\left(\frac{m}{10m+n}\right) = \left(\frac{2r}{20r+n}\right) = \left(\frac{2}{20r+n}\right)\left(\frac{r}{20r+n}\right)$$

$$= \left(\frac{2}{n+4}\right)\left(\frac{r}{n}\right) = -\left(\frac{2}{n}\right)\left(\frac{r}{n}\right) = -\left(\frac{2r}{n}\right) = -\left(\frac{m}{n}\right).$$

In either case $\chi(n + \mathfrak{f}/2) = -\chi(n)$ so

$$\sum_{n \pmod{\mathfrak{f}}} \chi(n)n = \sum_{n \pmod{\mathfrak{f}/2}} \chi(n)n + \chi(n + \mathfrak{f}/2)(n + \mathfrak{f}/2)$$

$$= \sum_{n \pmod{\mathfrak{f}/2}} \chi(n)n - \chi(n)(n + \mathfrak{f}/2) = -\mathfrak{f}/2 \sum_{n \pmod{\mathfrak{f}/2}} \chi(n).$$

The desired result is now immediate.

Using FORTRAN programs, we have computed h_2 for all values of $m < 2000$ where $m = p$ or $2p$ with p prime. In the tables above we list all such values of m with 5 dividing h_2. The type (or types) of each field was determined using the table of Ince [4] and a program to compute ϵ_2 (or ϵ_2 modulo 100 when overflow occurred in double precision) when $5m > 2025$. If Corollary 10 did not show $(h_2^*, 5) = 1$ and $m > 405$, then h_2^* was computed. This value appears in the tables whenever we computed it.

Department of Mathematics
Virginia Polytechnic Institute & State University
Blacksburg, Virginia 24061

1. H. HASSE, *Über die Klassenzahl abelscher Zahlkörper*, Akademie-Verlag, Berlin, 1952. MR 14, 141.

2. E. HECKE, *Vorlesungen über die Theorie der algebraischen Zahlen*, Leipzig, 1923.

3. C. S. HERZ, *Construction of Class Fields*, Lecture Notes in Math., vol. 21, Springer-Verlag, Berlin and New York, 1966. MR 34 #1278.

4. E. L. INCE, *Cycles of Reduced Ideals in Quadratic Fields*, British Math. Assn. Tables, Vol. 4, London, 1934.

5. T. KUBOTA, "Über die Beziehung der Klassenzahlen der Unterkörper des bizyklischen biquadratischen Zahlkörpers," *Nagoya Math. J.*, v. 6, 1953, pp. 119–127. MR 15, 605.

6. S. KURODA, "Über den Dirichletschen Körper," *J. Fac. Sci. Imp. Univ. Tokyo Sect. I*, v. 4, 1943, pp. 383–406. MR 9, 12.

7. C. PARRY, "Units of algebraic numberfields," *J. Number Theory*, v. 7, 1975, pp. 385–388. MR 52 #5625.

8. C. WALTER, *Class Number Relations in Algebraic Number Fields*, Ph.D. Thesis, University of Cambridge, 1976.

9. P. WEINBERGER, "Real quadratic fields with class numbers divisible by n," *J. Number Theory*, v. 5, 1973, pp. 237–241. MR 49 #252.

10. Y. YAMAMOTO, "On unramified galois extensions of quadratic number fields," *Osaka J. Math.*, v. 7, 1970, pp. 57–76. MR 42 #1800.