TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 190, 1974

CLASS NUMBERS OF REAL QUADRATIC NUMBER FIELDS

BY

EZRA BROWN

ABSTRACT. This article is a study of congruence conditions, modulo powers of two, on class number of real quadratic number fields $Q(\sqrt{d})$, for which d has at most three distinct prime divisors. Techniques used are those associated with Gaussian composition of binary quadratic forms.

1. Let $h(d)$ denote the class number of the quadratic field $Q(\sqrt{d})$ and let $h'(d)$ denote the number of classes of primitive binary quadratic forms of discriminant d [if $d < 0$ we count only positive forms]. It is well known [4] that $h(d) = h'(d)$, unless $d > 0$ and the fundamental unit ϵ of $Q(\sqrt{d})$ has norm 1, in which case $h(d) = \frac{1}{2}h'(d)$. Recently many authors have studied conditions on d under which a given power of two divides $h(d)$ (see [3, References]). Most of these articles deal with imaginary fields; in this article, we shall treat real fields for which d has at most three distinct prime divisors. Our method used to study this problem is the method of composition of forms, used in [1], [3]; we have included several known cases for the sake of completeness.

2. **Preliminaries.** A binary quadratic form is called ambiguous if its square, under Gaussian composition, is in the principal class, i.e. the class representing 1 (see [1] for explanations of any unfamiliar terminology). A class of forms is called ambiguous if it contains an ambiguous form. A form $[a, b, c] = ax^2 + bxy + cy^2$ is called ancipital if $b = 0$ or $b = a$. It was known to Gauss that the number of ambiguous classes of discriminant d equals the number of genera of discriminant d (see [7]), and that each ambiguous class of positive nonsquare discriminant contains exactly two ancipital forms with positive first coefficient (see [7]).

The primitive forms of discriminant d form an abelian group G of order $h'(d)$, the operation being composition and the identity being the principal class I. The principal genus G^+ is a subgroup of G consisting of all the classes which are squares under composition; the index of G^+ in G equals the number of genera. If d is the discriminant of a quadratic field, then d is fundamental, i.e. no square $s^2 > 1$ exists for which $d/s^2 \equiv 0$ or $1 \pmod 4$. Hence the number of genera

Received by the editors October 3, 1972.

AMS (MOS) subject classifications (1970). Primary 10A15, 10C05, 12A25, 12A50.

Key words and phrases. Class number, quadratic residues, quadratic fields, algebraic number fields, Gaussian composition, binary quadratic forms.

of a fundamental discriminant d is equal to $2^{\gamma+\theta-1}$, where γ is the number of distinct odd primes dividing d and $\theta = 0$ or 1 according as $d \equiv 1 \pmod 4$ or $d \equiv 8, 12 \pmod{16}$. (For proofs of any of the above statements, see [5].) Throughout this paper p, q and p_i denote odd primes and d is a fundamental discriminant; $(p|q)$ is the Legendre symbol, and we write $(p|q)_4 = 1$ or -1 according as p is or is not a biquadratic residue of q. If f and g are forms we write $f \sim g$ or $f \not\sim g$ according as f is or is not equivalent to g.

3. **Discriminants with one prime divisor.** If d is a positive discriminant with exactly one prime divisor, then there is only one genus; this genus contains the one ambiguous class, namely I, and several pairs of improperly equivalent nonambiguous classes. Thus, $h'(d)$ is odd; it is impossible that $h(d) = \frac{1}{2}h'(d)$, so that $h(d) = h'(d)$, the norm $N\epsilon$ of the fundamental unit is -1, and $h(d)$ is odd.

4. **The case $d = 4p$ or $d = 8p$.** If $d = 4p$ is fundamental, then $p \equiv 3 \pmod 4$; there are two genera, hence two ambiguous classes. Since $N\epsilon = +1$, the ambiguous classes are I and $-I$, and $-I$ contains the form $f_{-1} = [p, 0, -1]$; since $(f_{-1} \mid p) = -1$, $-I \notin G^+$. Hence each genus contains an ambiguous class and several pairs of improperly equivalent nonambiguous classes. Since each genus always contains the same number of classes, we deduce that $h'(4p) \equiv 2 \pmod 4$ and hence $h(4p)$ is odd. Similarly, if $d = 8p$ and $p \equiv 3 \pmod 4$, there are two genera; the ambiguous classes are I and $-I$, distributed one to each genus. Hence $h'(8p) \equiv 2 \pmod 4$ and $h(8p)$ is odd.

Let $d = 8p$ with $p \equiv 1 \pmod 4$. The four ancipital forms with positive first coefficient are $f_1 = [1, 0, -2p]$, $f_{-1} = [2p, 0, -1]$, $f_2 = [2, 0, -p]$ and $f_{-2} = [p, 0, -2]$, and the generic invariants are $(m \mid p)$ and $(2 \mid m)$. If $p \equiv 5 \pmod 8$, then $(f_2|p) = (f_{-2}|p) = -1$, so that $f_2 \notin G^+$ and the ambiguous classes are distributed one to each genus. As above, we deduce that $h'(8p) = 2 \pmod 4$; however, $f_2 \notin G^+$ imply that $f_1 \sim f_{-1}$, so that $N\epsilon = -1$. Hence $h(8p) = h'(8p) \equiv 2 \pmod 4$.

Let $d = 8p$, $p \equiv 1 \pmod 8$. Then both ambiguous classes lie in the principal genus. Denote by N the nonprincipal ambiguous class: since $N \in G^+$, $N = D^2$ for some class D, and thus D has order 4 in G. If we let $H = \{D, N = D^2, D^3, I = D^4\}$, then $h'(8p) = \operatorname{ord} G = \operatorname{ord}(G/H) \cdot \operatorname{ord} H \equiv 0 \pmod 4$. Now $p \equiv 1 \pmod 8$ so there exist positive integers a, b, e and f such that $p = a^2 + 2b^2 = 2f^2 - e^2$. Let $g_{-2} = [a, 4b, -2a]$ and let $g_2 = [e, 4f, 2e]$; then $g_{-2}^2 \sim f_{-2}$ and $g_2^2 \sim f_2$. It is clear that g_{-2} has order 4 whenever $f_{-2} \in N$ and g_2 has order 4 whenever $f_2 \in N$. Hence $g_{-2} \in D$ or D^3 if $f_{-2} \in N$, and $g_2 \in D$ or D^3 if $f_2 \in N$. If $D \in G^+$, then $h'(8p) \equiv 0 \pmod 8$, since $h'(8p) = \operatorname{ord}(G/G^+) \cdot \operatorname{ord}(G^+/H) \cdot \operatorname{ord} H = 2 \cdot \operatorname{ord}(G^+H) \cdot 4 \equiv 0 \pmod 8$. If $D \notin G^+$, let B be a class for which $B^2 \in H$. Now $B^2 \neq D$ or D^3, since D and D^3 are not squares. If $B^2 = N$, then $B^2D^2 = N^2 = I$, so that $BD = I$ or N, i.e., $B = D^3$ or D. If $B^2 = I$, then $B = N$ or I. Hence the index of H in G is odd i.e. $h'(8p) = \operatorname{ord}(G/H) \cdot \operatorname{ord} H \equiv 4 \pmod 8$.

Now $g_{-2} \in G^+$ if and only if $a \equiv \pm 1 \pmod 8$ and $g_2 \in G^+$ if and only if $e \equiv \pm 1 \pmod 8$. In addition, $\pm e \equiv 1$ or $3 \pmod 8$ according as $p \equiv 1$ or $9 \pmod{16}$.

Case (a): $p \equiv 9 \pmod{16}$. By Pall [7], $f_1 \sim f_{-1}$ if and only if $b \equiv 0 \pmod 4$ and $f_1 \sim f_{-2}$ if and only if $b \equiv 2 \pmod 4$. Hence, $f_2 \in N$ and $g_2 \in D$; but $\pm e \equiv 3 \pmod 8$, so that $D \notin G^+$. Thus, if $b \equiv 0 \pmod 4$, then $N\epsilon = -1$ and $h(8p) = h'(8p) \equiv 4 \pmod 8$; if $b \equiv 2 \pmod 4$, then $N\epsilon = +1$ and $h(8p) = \frac{1}{2}h'(8p) \equiv 2 \pmod 4$.

Case (b): $p \equiv 1 \pmod{16}$. Now $\pm a \equiv 1$ or $3 \pmod 8$ according as $b \equiv 0$ or $2 \pmod 4$. By Pall [7], if $b \equiv 2 \pmod 4$, then $f_1 \sim f_2$; in that case, $f_{-2} \in N$, $g_{-2} \in D$ and $\pm a \equiv 3 \pmod 8$, so that $D \notin G^+$ and $h'(8p) \equiv 4 \pmod 8$. Since $f_1 \not\sim f_{-1}$, $h(8p) \equiv 2 \pmod 4$. If $b \equiv 0 \pmod 4$, any of f_{-1}, f_2 and f_{-2} may be in I: since $\pm a \equiv 1$ and $\pm e \equiv 1 \pmod 8$, $D \in G^+$ and $h'(8p) \equiv 0 \pmod 8$. Hence $h(8p) \equiv 0 \pmod 4$ unless $f_1 \sim f_{-1}$, in which case $h(8p) \equiv 0 \pmod 8$.

Thus we have proved the following theorem.

Theorem 1. *Let p be an odd prime.*

(a) *If $p \equiv 3 \pmod 4$, then $h'(4p) \equiv h'(8p) \equiv 2 \pmod 4$ and $h(4p) \equiv h(8p) \equiv 1 \pmod 2$.*

(b) *If $p \equiv 5 \pmod 8$, then $h(8p) = h'(8p) \equiv 2 \pmod 4$.*

(c) *If $p \equiv 1 \pmod 8$, write $p = a^2 + 2b^2$ with a and b positive integers. If $p \equiv 1 \pmod{16}$ and $b \equiv 0 \pmod 4$, then $h'(8p) \equiv 0 \pmod 8$; otherwise, $h'(8p) \equiv 4 \pmod 8$.*

(d) *If $p \equiv 9 \pmod{16}$, then $h(8p) \equiv 4 \pmod 8$ or $h(8p) \equiv 2 \pmod 4$ according as $b \equiv 0$ or $2 \pmod 4$.*

(e) *If $p \equiv 1 \pmod{16}$, then $h(8p) \equiv 2 \pmod 4$ if $b \equiv 2 \pmod 4$; however, if $b \equiv 0 \pmod 4$, then $h(8p) \equiv 0 \pmod 4$ or 8 according as $x^2 - 2py^2 = -1$ does not or does have a solution in integers.*

Remark. If f_{-2} is a fourth power, then $g_{-2} \in G^+$, i.e. $(a \mid p) = (2 \mid a) = 1$. Since $f_{-2} \sim g_{-2}^2$, we may write $a^2 = px^2 - 2y^2$ where x is odd, $y = 2^\alpha y'$, $\alpha > 1$ and y' is odd. Hence we have that

$$(2 \mid a) = (a \mid p) = (-1 \mid p)_4 (2 \mid p)_4 (2 \mid p)^\alpha (y' \mid p) = (2 \mid p)_4,$$

since $p \equiv 1 \pmod 8$ and $(p \mid y') = 1$. Thus f_{-2} is a fourth power if and only if $(2 \mid p)_4 \,(= (2 \mid a)) = 1$. It is then straightforward to verify that

$$(2 \mid p)_4 = (-1)^{(p-1)/8 + b/2},$$

which is one form of a result due to Dirichlet [7].

5. **The case $d = pq$, $p \equiv q \pmod 4$.** We shall prove the following:

Theorem 2. *Let $p \equiv q \pmod 4$ be distinct odd primes. The congruence conditions on $h(pq)$ and $h'(pq)$ modulo powers of 2 are given by the following table.*

p and q	$h'(pq) \pmod m$	$h(pq) \pmod m$
$p \equiv q \equiv 3 \pmod 4$	$2 \pmod 4$	$1 \pmod 2$
$p \equiv q \equiv 1 \pmod 4$:	$2 \pmod 4$	$2 \pmod 4$
$(p\|q) = -1$		
$(p\|q) = 1$:		
$(p\|q)_4 = (q\|p)_4 = -1$	$4 \pmod 8$	$4 \pmod 8$
$(p\|q)_4(q\|p)_4 = -1$	$4 \pmod 8$	$2 \pmod 4$
$(p\|q)_4 = (q\|p)_4 = 1$	$0 \pmod 8$	$0 \pmod 8$ *if* $N\epsilon = -1$;
		$0 \pmod 4$ *if* $N\epsilon = 1$.

Proof. It is known [6] that $h'(pq)$ and $h'(4pq)$ are exactly divisible by the same power of 2 if $p \equiv q \pmod 4$; the forms of discriminant $4pq$ are easier to treat, so we will use them to get results on discriminant pq. There are two genera, hence two ambiguous classes, and the four ancipital forms with positive first coefficients are $f_1 = [1, 0, -pq]$, $f_{-1} = [pq, 0, -1]$, $f_p = [p, 0, -q]$ and $f_{-p} = [q, 0, -p]$.

If $p \equiv q \equiv 3 \pmod 4$, then $f_{-1} \notin G^+$, and if $p \equiv q \equiv 1 \pmod 4$ and $(p \mid q) = -1$, then $f_1 \sim f_{-1}$ and $f_p \notin G^+$. Hence the ambiguous classes are distributed one to a genus and we have $h'(pq) \equiv 2 \pmod 4$. If $p \equiv q \equiv 3 \pmod 4$, then $f_{-1} \not\sim f_1$, so that $h(pq)$ is odd; if $p \equiv q \equiv 1 \pmod 4$ and $(p \mid q) = -1$, then $h(pq) = h'(pq) \equiv 2 \pmod 4$.

If $p \equiv q \equiv 1 \pmod 4$ and $(p \mid q) = 1$, then both ambiguous classes are in the principal genus, so that $h'(pq) \equiv 0 \pmod 4$. Now $f_p \in G^+$, so there is a form g_p with leading coefficient r prime to $2pq$ such that $f_p \sim g_p^2$, whence f_p represents r^2. Hence f_p is a fourth power exactly when $(r \mid p) = (r \mid q) = 1$. Writing $r^2 = px^2 - qy^2$, we see that x is odd, $y = 2^\alpha y'$, $\alpha > 0$, y' is odd and $\alpha = 1$ if and only if $p \equiv 5 \pmod 8$; furthermore, $(p \mid y') = 1$ and $(-1 \mid p)_4 = (2 \mid p)$ whenever $p \equiv 1 \pmod 4$. Hence $(r \mid p) = (q \mid p)_4 (2 \mid p)^{\alpha+1} (y' \mid p) = (q \mid p)_4$, and hence f_p is a fourth power if and only if $(q \mid p)_4 = 1$. Similarly, f_{-p} is a fourth power if and only if $(p \mid q)_4 = 1$. Since $h'(pq) \equiv 0 \pmod 4$, f_1 is a fourth power, which implies that $N\epsilon = -1$ if $(p \mid q)_4 = (q \mid p)_4 = -1$.

If $(p \mid q)_4 (q \mid p)_4 = -1$, then exactly one of f_p and f_{-p} is a fourth power, that one is in I, and hence $f_{-1} \notin I$. Thus, $f_1 \sim f_p$ if $(q \mid p)_4 = 1 = -(p \mid q)_4$, and $f_1 \sim f_{-p}$ if $(p \mid q)_4 = 1 = -(q \mid p)_4$ (for an alternate proof of this, see [2]).

Furthermore, if $(p \mid q)_4 = -1$ or $(q \mid p)_4 = -1$, then $h'(pq) \equiv 4 \pmod 8$. To see this, let D be a class such that $D^2 = N$, the nonprincipal ambiguous class. If $(p \mid q)_4 = -1$ or $(q \mid p)_4 = -1$, then $D \notin G^+$ by the above, so that neither D nor D^3

is a square. As in the proof of Theorem 1, it is straightforward to verify that $H = \{I, D, D^2, D^3\}$ has odd index in G, i.e. $h'(pq) \equiv 4 \pmod 8$.

Finally, if $(p \mid q)_4 = (q \mid p)_4 = 1$, then $H \subseteq G^+$, so that $h'(pq) \equiv \operatorname{ord} G \equiv \operatorname{ord}(G/G^+) \cdot \operatorname{ord}(G^+/H) \cdot \operatorname{ord} H \equiv 2 \cdot \operatorname{ord}(G^+/H) \cdot 4 \equiv 0 \pmod 8$. Hence $h(pq) \equiv 0 \pmod 8$ if $N\epsilon = -1$ and $h(pq) \equiv 0 \pmod 4$ if $N\epsilon = 1$. We are done.

Remark. There still remains open the difficult case $(p \mid q)_4 = (q \mid p)_4 = 1$. One possible approach is the following: since $h'(pq) \equiv 0 \pmod 8$, $D \in G^+$, so that D represents an odd square r^2 prime to pq, where r is represented by B and $B^2 = D$. Then it is easily shown that $h'(pq) \equiv 0 \pmod{16}$ if and only if $B \in G^+$, i.e. $(r \mid p) = (r \mid q) = 1$. Now we have $r^2 = kx^2 + 2mxy + ny^2$, where $[k, 2m, n] \in D$; perhaps examining this equation modulo p would yield results. A similar remark applies to the case $p \equiv 1 \pmod{16}$ and $b \equiv 0 \pmod 4$ for discriminants $d = 8p$.

6. **The case $d = 4pq$, $p \not\equiv q \pmod 4$.** Let $p \equiv 1 \equiv -q \pmod 4$. There are four ambiguous classes: Since $d \equiv 12 \pmod{16}$, the generic characters are $(m \mid p)$, $(m \mid q)$ and $(-1 \mid m)$. Since $f_{-1} = [pq, 0, -1]$ satisfies $(-1 \mid f_1) = -1$, $f_{-1} \notin G^+$, so that $N\epsilon = +1$ and $h(4pq) = \frac{1}{2}h'(4pq)$. The other ancipital forms are f_1, f_p and f_{-p} of §5, and $f_2 = [2, 2, \frac{1}{2}(1 - pq)]$, $f_{-2} = [\frac{1}{2}(pq - 1), -2, -2]$, $f_{2p} = [2p, 2p, \frac{1}{2}(p - q)]$ and $f_{2q} = [2q, 2q, \frac{1}{2}(q - p)]$. We construct a table of generic characters (from the Gauss product relation, we know that $(-1 \mid m) = (m \mid p)(m \mid q)$):

	$(m\|p)$	$(m\|q)$
f_1	1	1
f_{-1}	1	-1
f_p	$(p\|q)$	$(p\|q)$
f_{-p}	$(p\|q)$	$-(p\|q)$
f_2	$(2\|p)$	$(2\|q)$
f_{-2}	$(2\|p)$	$-(2\|q)$
f_{2p}	$(2\|p)(p\|q)$	$(2\|q)(p\|q)$
f_{2q}	$(2\|p)(p\|q)$	$-(2\|q)(p\|q)$

From this table, it is evident that if $(p \mid q) = 1$, then f_1, f_{-1}, f_p and f_{-p} are all in different genera; in addition, if $p \equiv 5 \pmod 8$, then f_1, f_{-1}, f_2 and f_{-2} are all in different genera. In those cases, each of the four genera contains an odd number of classes: hence $h'(4pq) = 4 \pmod 8$ and $h(4pq) = 2 \pmod 4$.

Let $p \equiv 1 \pmod 8$ and $(p \mid q) = 1$. Then f_1 and $f_p \in G^+$; in addition, f_{-2} and $f_{2q} \in G^+$ if $q \equiv 3 \pmod 8$, and f_2 and $f_{2p} \in G^+$ if $q \equiv 7 \pmod 8$. Thus G^+ has even order and hence $h'(4pq) = \operatorname{ord} G^+ \cdot \operatorname{ord}(G/G^+) \equiv 0 \pmod 8$. If f_p is to be a

fourth power, then there exists a form g_p such that $f_p \sim g_p^2$ and $g_p \in G^+$: this can happen if and only if $(r \mid p) = (r \mid q) = (-1 \mid r) = 1$, where r is primitively represented by g_p. If r is such a number, we may write $r^2 = px^2 - qy^2$, where $y = 2^\alpha y'$ and y' is odd: then $(r \mid p) = (-1 \mid p)_4 (q \mid p)_4 (2 \mid p)^\alpha (y' \mid p) = (q \mid p)_4$. [*Note*: We cannot do this mod q since $(m \mid q)_4 = (m \mid q)$; also, the condition $(-1 \mid r) = 1$ is of no use.] Hence, if f_p is a fourth power, then $(q \mid p)_4 = 1$; thus, if $p \equiv 1 \pmod 8$, $(p \mid q) = 1$ and $(q \mid p)_4 = -1$, then $f_1 \not\sim f_p$, since f_1 is always a fourth power; by the group-theoretic arguments previously used, we deduce that $h'(4pq) \equiv 8 \pmod{16}$.

Let $q \equiv 3 \pmod 8$ and write $pq = f^2 + 2e^2$. The form $g_{-2} = [e, 2f, -2e]$ satisfies $g_{-2}^2 \sim f_{-2}$. Hence f_{-2} is a fourth power if and only if $(e \mid p) = (-1 \mid e) = 1$ (note that $(p \mid q) = (e \mid p)(-1 \mid e)$). Since $[-e, 2f, -2(-e)]^2 \sim f_{-2}$, we may assume that $e \equiv 1 \pmod 4$. Thus, f_{-2} is a fourth power if and only if $pq = f^2 + 2e^2$, where $e \equiv 1 \pmod 4$ and $(e \mid p) = 1$. Similarly, if $q \equiv 7 \pmod 8$, it can be shown that f_2 is a fourth power if and only if $pq = f^2 - 2e^2$ where $e \equiv 1 \pmod 4$ and $(e \mid p) = 1$. Thus, by the group-theoretic arguments previously used, we deduce that if $q \equiv 3(7) \pmod 8$ and $f_1 \not\sim f_{-2}(f_2)$, then $h'(4pq) \equiv 0$ or $8 \pmod{16}$ according as $pq = f^2 + 2e^2$ $(pq = f^2 - 2e^2)$ with $(e \mid p) \equiv 1 \equiv e \pmod 4$ or not. Finally, we observe that $f_1 \sim f_p$ or $f_1 \sim f_{\pm 2}$, but not both. We thus have the following theorem.

Theorem 3. (a) *Let* $p \equiv 1 \equiv -q \pmod 4$ *be primes; then* $h(4pq) = \frac{1}{2} h'(4pq)$. *If* $p \equiv 5 \pmod 8$ *or if* $(p \mid q) = -1$, *then* $h'(4pq) \equiv 4 \pmod 8$; *otherwise* $h'(4pq) \equiv 0 \pmod 8$.

(b) *Let* $p \equiv 1$, $q \equiv 3(7) \pmod 8$ *and* $(p \mid q) = 1$; *write* $pq = f^2 + 2e^2 (f^2 - 2e^2)$ *with* $e \equiv 1 \pmod 4$. *If* $(e \mid p) = -1$ *or if* $(q \mid p)_4 = -1$, *then* $h'(4pq) \equiv 8 \pmod{16}$. *If* $x^2 - pqy^2 = -2(+2)$ *has no solutions and* $(e \mid p) = 1$, *then* $h'(4pq) \equiv 0 \pmod{16}$.

7. **The case** $d = 8pq$. There are four genera and the eight ancipital forms with positive first coefficients are as follows:

$$f_1 = [1, 0, -2pq], \qquad f_{-1} = [2pq, 0, -1],$$

$$f_2 = [2, 0, -pq], \qquad f_{-2} = [pq, 0, -2],$$

$$f_p = [p, 0, -2q], \qquad f_{-p} = [2q, 0, -p],$$

$$f_q = [q, 0, -2p], \qquad f_{-q} = [2p, 0, -q].$$

If we construct a table of generic characters, we then deduce the following information:

p(mod 8)	q(mod 8)	Ancipital forms f_i in G^+	
		$(p\|q) = -1$	$(p\|q) = 1$
1	1	$f_{\pm 1}, f_{\pm 2}$	All
1	5	$f_{\pm 1}$	$f_{\pm 1}, f_{\pm p}$
5	5	$f_{\pm 1}$	$f_{\pm 1}$
3	3	f_1, f_{-2}	f_1, f_{-2}
3	7	f_1, f_q	f_1, f_{-q}
7	7	f_1, f_2, f_{-p}, f_q	f_1, f_2, f_{-p}, f_{-q}
1	3	f_1, f_{-2}	f_1, f_{-2}, f_p, f_q
1	7	f_1, f_2	f_1, f_2, f_p, f_{-q}
5	3	f_1, f_{-p}	f_1, f_q
5	7	f_1, f_{-p}	f_1, f_{-q}

From this we observe that G^+ contains all four ambiguous classes if $(p \mid q) = 1 \equiv p \equiv q \pmod 8$; two ambiguous classes if (a) $p \equiv q \equiv 7 \pmod 8$, (b) $p \equiv q \equiv 1 \pmod 8$ and $(p \mid q) = -1$, or (c) $p \equiv 1 \not\equiv q \pmod 8$ and $(p \mid q) = 1$; one ambiguous class in all other cases. By using the same techniques as we used in the previous sections we may prove the following lemma (the painful but elementary details are omitted).

Lemma. (1) *Let* $p \equiv 1 \pmod 8$ *and suppose* $(p \mid q) = 1$. *If* f_p *is a fourth power, then* $(2 \mid p)_4 = (q \mid p)_4$.

(2) *Let* $p \equiv 1 \pmod 8$, $q \equiv 1 \pmod 4$ *and* $(p \mid q) = 1$. *If* f_{-p} *is a fourth power, then* $(p \mid q)_4 = 1$ *or* -1 *according as* $p \equiv 1$ *or* $9 \pmod{16}$.

(3) *Let* $p \equiv 1$ *and* $q \equiv 1$ *or* $3 \pmod 8$; *write* $pq = e^2 + 2f^2$ *with* $e \equiv 1 \pmod 4$. *Then* f_{-2} *is a fourth power if and only if* $(e \mid p) = (e \mid q) = 1$.

(4) *Let* $p \equiv 1 \equiv \pm q \pmod 8$; *write* $pq = 2f^2 - e^2$ *with* $e \equiv 1 \pmod 4$. *Then* f_2 *is a fourth power if and only if* $(e \mid p) = (e \mid q) = 1$.

As a consequence of the lemma and the table of ancipital forms, we may deduce the following theorem.

Theorem 4. (a) *Let* $p \equiv q \equiv 1 \pmod 8$ *and* $(p \mid q) = 1$. *Then all four ambiguous classes are in* G^+, *so* $b'(8pq) \equiv 0 \pmod{16}$. *Write* $pq = 2f^2 - e^2 = 2b^2 + a^2$ *with* $a \equiv e \equiv 1 \pmod 4$. *If* $(a \mid p) = (a \mid q) = (e \mid p) = (e \mid q) = 1$, *then* $b'(8pq) \equiv 0 \pmod{32}$. *If each of the following conditions holds then* $N\epsilon = -1$ and $b(8pq) = b'(8pq) \equiv 16 \pmod{32}$:

(i) $(a \mid p) = -1$ *or* $(a \mid q) = -1$;
(ii) $(e \mid p) = -1$ *or* $(e \mid q) = -1$;
(iii) $(2 \mid p)_4 \neq (q \mid p)_4$;
(iv) $(2 \mid q)_4 \neq (p \mid q)_4$;
(v) $(p \mid q)_4 = (-1)^{(p+7)/8}$; *and*
(vi) $(q \mid p)_4 = (-1)^{(q+7)/8}$.

Otherwise, we have no information.

(b) *Let* $p \equiv q \equiv 1 \pmod 8$ *and* $(p \mid q) = -1$; *write* $pq = 2f^2 - e^2 = 2b^2 + a^2$ *with* $a \equiv e \equiv 1 \pmod 4$. *If* $(a \mid p) = (a \mid q) = (e \mid p) = (e \mid q) = 1$, *then* $h'(8pq) \equiv 0 \pmod{16}$; *otherwise,* $h'(8pq) \equiv 8 \pmod{16}$. *If* (i) $(a \mid p) = -1$ *or* $(a \mid q) = -1$, *and* (ii) $(e \mid p) = -1$ *or* $(e \mid q) = -1$, *then* $N\epsilon = -1$ *and* $h(8pq) = h'(8pq) \equiv 8 \pmod{16}$. *Otherwise,* $h'(8pq) \equiv 0 \pmod 8$.

(c) *Let* $p \equiv 1$ *and* $q \equiv 3$ $(q \equiv 7) \pmod 8$ *and* $(p \mid q) = 1$; *write* $pq = 2f^2 + e^2(2f^2 - e^2)$ *with* $e \equiv 1 \pmod 4$. *Then* $N\epsilon = 1$. *If* $(e \mid p) = -1$ *or* $(e \mid q) = -1$ *or* $(2 \mid p)_4 \neq (q \mid p)_4$, *then* $h'(8pq) \equiv 8 \pmod{16}$; *if* $f_1 \sim f_p$ *or* $f_1 \sim f_q$ ($f_1 \sim f_p$ *or* $f_1 \sim f_{-q}$) *and if* $(e \mid p) = (e \mid q) = 1$, *then* $h'(8pq) \equiv 0 \pmod{16}$. *Otherwise we have no information, except that* $h'(8pq) \equiv 0 \pmod 8$.

(d) *Let* $p \equiv 1$, $q \equiv 5 \pmod 8$ *and* $(p \mid q) = 1$. *If* $(2 \mid p)_4 \neq (q \mid p)_4$ *or if* $(p \mid q)_4 = (-1)^{(p+7)/8}$, *then* $h'(8pq) \equiv 8 \pmod{16}$; *if both of these conditions occur, then* $N\epsilon = -1$ *and* $h(8pq) \equiv 8 \pmod{16}$. *If neither occurs, then* $h'(8pq) \equiv 0 \pmod 8$.

(e) *Let* $p \equiv q \equiv 7 \pmod 8$; *then* $N\epsilon = 1$ *and* $h'(8pq) \equiv 0 \pmod 8$.

The proof of this theorem relies on group-theoretic arguments similar to those used in the proofs of previous theorems. Conditions (a)(i) through (a)(vi) imply that the only ancipital forms which are fourth powers are f_1 and f_{-1}; hence $f_1 \sim f_{-1}$ and $N\epsilon = -1$. The other statements are easily verified, so we omit the remainder of the proof. Within the limitations of our techniques, it appears that our results are best possible.

8. **The case $d = p_1p_2p_3$, p_i odd primes.** Since $d \equiv 1 \pmod 4$ we may assume that $p_1 \equiv 1$ and $p_2 \equiv p_3 \pmod 4$. We will simply state the results, as the proofs are obtained in precisely the same manner as were the previous proofs.

Theorem 5. (a) *Let* $p_1 \equiv 1$ *and* $p_2 \equiv p_3 \equiv 3 \pmod 4$. *Then* $N\epsilon = 1$ *and* $h'(p_1p_2p_3) \equiv 0$ *or* $4 \pmod 8$ *according as* $(p_1 \mid p_2) = (p_1 \mid p_3) = 1$ *or not. If* $(p_1 \mid p_2) = (p_1 \mid p_3) = 1$ *and* $(p_2 \mid p_1)_4 \neq (p_3 \mid p_1)_4$, *then* $h'(p_1p_2p_3) \equiv 8 \pmod{16}$; *otherwise we have no information.*

(b) *Let* $p_i \equiv 1 \pmod 4$, $i = 1, 2, 3$. *Then* $h'(p_1p_2p_3) \equiv 0$ *or* $4 \pmod 8$ *according as at most one or at least two of the symbols* $\{(p_1 \mid p_2), (p_1 \mid p_3), (p_2 \mid p_3)\}$ *equal* -1; *if they are all equal to* 1, *then* $h'(p_1p_2p_3) \equiv 0 \pmod{16}$.

(c) *Let* $p_i \equiv 1 \pmod 4$, $i = 1, 2, 3$, $(p_1 \mid p_2) = (p_1 \mid p_3) = 1$ *and* $(p_2 \mid p_3) = -1$. *If either* $(p_2 \mid p_1)_4 \neq (p_3 \mid p_1)_4$ *or* $(p_1 \mid p_2)_4 \neq (p_1 \mid p_3)_4$ *then* $h'(p_1p_2p_3) \equiv 8 \pmod{16}$,

and if both relations hold, then $N\epsilon = -1$ *and* $h(p_1p_2p_3) \equiv 8 \pmod{16}$. *Otherwise we have no information.*

(d) *Let* $p_i \equiv 1 \pmod 4$, $i = 1, 2, 3$ *and* $(p_i|p_j) = 1$ *for* $i \neq j$. *If* $(p_i|p_j)_4(p_i|p_k)_4 = (p_j|p_i)_4(p_k|p_i)_4 = -1$ *for* i, j *and* k *distinct, then* $h'(p_1p_2p_3) \equiv 16 \pmod{32}$ *and* $N\epsilon = -1$. *Otherwise we have no further information.*

Remark. The difficulty in obtaining further information in Theorems 4 and 5 stems from the fact that certain given conditions on fourth power residue symbols are necessary, but not sufficient, for certain ambiguous classes to be fourth power.

9. **A problem.** The techniques of this paper have been used to treat imaginary fields with two or three divisors of the discriminant [1], [3] and clearly may be used to treat arbitrary quadratic fields. In each of the theorems of this and previous papers on the subject, there are open cases. What can be said about these cases?

REFERENCES

1. Ezra Brown, *The class number of* $Q(\sqrt{-p})$ *for* $p \equiv 1 \pmod 8$ *a prime*, Proc. Amer. Math. Soc. 31 (1972), 381–383. MR 44 #6645.

2. ———, *Binary quadratic forms of determinant* $-pq$, J. Number Theory 4 (1972), 408–410. MR 46 #134.

3. ———, *Class numbers of complex quadratic fields*, J. Number Theory (to appear).

4. Harvey Cohn, *A second course in number theory*, Wiley, New York, 1962. MR 24 #A3115.

5. Burton W. Jones, *The arithmetic theory of quadratic forms*, Carus Monograph Series, no. 10, The Math. Assoc. of America, Buffalo, N. Y., 1950. MR 12, 244.

6. Gordon Pall, *Binary quadratic discriminants differing by square factors*, Amer. J. Math. 57 (1935), 789–799.

7. ———, *Discriminantal divisors of binary quadratic forms*, J. Number Theory 1 (1969), 525–533. MR 40 #1335.

DEPARTMENT OF MATHEMATICS, VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY, BLACKSBURG, VIRGINIA 24061