PACIFIC JOURNAL OF MATHEMATICS
Vol. 108, No. 1, 1983

THE QUADRATIC NUMBER FIELDS WITH CYCLIC 2-CLASSGROUPS

PATRICK MORTON

Many authors have considered the divisibility of the restricted class number $h^+(d)$ of the quadratic field $\Omega = Q(\sqrt{d})$ by 4 and 8, in the case that the discriminant d of Ω has exactly two prime factors. For such discriminants the restricted classgroup $\mathcal{C}$ of Ω has a nontrivial cyclic 2-Sylow subgroup, and conditions on d can be given for the existence of classes in $\mathcal{C}$ of orders 4 and 8. The first such results are due to Rédei.

In this paper we give criteria for the divisibility of $h^+(d)$ by 8 which are phrased in terms of the splitting of one of the prime factors p of d in a normal extension of Q depending only on $d/p = d_0$. This simplifies and unifies the criteria for $8 \mid h^+(d)$ existing in the literature, which depend mainly in the representation of the prime p by certain quadratic forms, or on the quadratic character of solutions to ternary quadratic equations.

1. Introduction. We start from the Rédei-Reichardt theorem [**25**], [**20**], which asserts that $4 \mid h^+(d)$ if and only if d has one of the following forms:

(a) $d = -4p$, or $8p$, $p \equiv 1 \pmod 8$;
(b) $d = -8p$, $p \equiv \pm 1 \pmod 8$;
(c) $d = qp^*$, $q \equiv 1 \pmod 4$, p odd, $p^* = (-1)^{(p-1)/2}p$, and $(p/q) = +1$.

(p and q are primes.) We then deduce our criteria for $8 \mid h^+(d)$ by a simple application of quadratic reciprocity. Since our theorems are phrased in terms of the splitting of primes, the Frobenius density theorem gives as immediate corollaries results concerning the density of p for which $8 \mid h^+(d)$. For example, the density of primes p for which $8 \mid h(-4p)$ is $1/8$. (Here $h(d)$ denotes the absolute class number.) Similar techniques are also applicable to fields $\Omega = Q(\sqrt{d})$ with d a product of any number of primes. In [**21**], [**22**] we use these techniques to simplify and extend results of Rédei [**27**], [**28**].

Moreover, as by-products of our proofs we get several known results in a very simple fashion, among which are a relation between $h^+(8p)$, $h(-4p)$ and $h(-8p)$ (see Theorem 4), and a result of E. Lehmer [**19**] related to quartic reciprocity. The latter result is closely connected with a certain abelian quartic field, whose rational character occurs naturally in the discussion of case (c). (See §4.)

In analogy to the above fact concerning the divisibility of $h(-4p)$ by 8, it appears from computations by several authors **[6]**, **[17]** that the density of primes p for which $16 \mid h(-4p)$ is $1/16$. This raises the question: can these primes be characterized by their behavior in some normal extension of Q? The existence of such an extension would explain the apparent density $1/16$. However, Cohn and Lagarias **[5]**, **[6]** have shown that this hypothetical field is not to be found easily. More specifically, they have shown that no field of degree 16 ramified only over 2 can characterize the divisibility of $h(-4p)$ by 16. Of course the same question can be asked for other powers of 2. We refer the reader to **[5]**, **[6]** for further discussion of the relevant conjectures.

I would like to take this opportunity to express my gratitude to Jeff Lagarias, who suggested using normal extensions in studying $h^+(d)$, and with whom I have had many stimulating conversations.

2. Preliminaries. Let the prime factors of the discriminant d of $\Omega = Q(\sqrt{d})$ be p and q, where $q = 2$ if d is even. Then by the genus theory of Gauss the restricted 2-classgroup of Ω is cyclic. (Recall that ideal classes are defined by strict equivalence, so $\mathfrak{a} \sim \mathfrak{b}$ if and only if $\mathfrak{a} = (\gamma)\mathfrak{b}$ with $\operatorname{Norm}\gamma > 0$, and that the 2-classgroup is simply the 2-Sylow subgroup of the resulting classgroup.) Moreover the unique nontrivial class of order 2 contains one of the ideals $\mathfrak{p}$, $\mathfrak{q}$, or $\mathfrak{p}\mathfrak{q}$, where

$$\mathfrak{p}^2 = (p) \quad \text{and} \quad \mathfrak{q}^2 = (q).$$

(We refer the reader to **[14]** and **[20]** for details.) Since an ideal $\mathfrak{a}$ lies in the square of some ideal class if and only if the common value of the Hilbert symbols

$$\chi(\mathfrak{a}) = \left(\frac{N\mathfrak{a}, d}{p}\right) = \left(\frac{N\mathfrak{a}, d}{q}\right) \tag{1}$$

is one (here N denotes the norm), it follows that 4 divides the restricted class number $h^+(d)$ exactly when

$$\chi(\mathfrak{p}) = \chi(\mathfrak{q}) = 1.$$

This is easily seen to happen if and only if d has the form (a), (b), or (c) if §1.

Henceforth we assume d has one of these forms, and we ask when $8 \mid h^+(d)$. Both ideals $\mathfrak{p}$ and $\mathfrak{q}$ are now equivalent to squares:

$$\mathfrak{p} \sim \mathfrak{z}^2, \qquad \mathfrak{q} \sim \mathfrak{w}^2, \tag{2}$$

and $\mathfrak{z}$, $\mathfrak{w}$ generate the classes of order 4. Hence $8 \mid h^+(d)$ if and only if

$$\chi(\mathfrak{z}) = \chi(\mathfrak{w}) = 1. \tag{3}$$

The computation of $\chi(\mathfrak{z})$ and $\chi(\mathfrak{w})$ depends on the following lemma. (Cf. [**30**].)

LEMMA 1. *Let* $\mathfrak{a} = \mathfrak{p}$ *or* $\mathfrak{q}$, $a = N\mathfrak{a}$. *If* (x, y, z) *is a positive primitive solution of*

$$x^2 - dy^2 - 4az^2 = 0, \tag{4}$$

then there is an ideal $\mathfrak{b}$ *for which* $\mathfrak{b}^2 \sim \mathfrak{a}$ *and* $N\mathfrak{b} = z$.

Proof. Let γ denote the integer $(x + y\sqrt{d})/2$. Then γ is primitive, i.e. divisible by no rational prime, by the primitivity of the solution (x, y, z) and the fact that a is square-free. If γ' denotes the conjugate of γ, it follows from $N\gamma = \gamma\gamma' = az^2$ that $(\gamma, \gamma') = \mathfrak{a}$, and so

$$(\gamma) = \mathfrak{a}\mathfrak{b}^2, \quad \text{where } N\mathfrak{b} = z.$$

But then $\mathfrak{b}^2 \sim \mathfrak{b}^2\mathfrak{a}^2 = \mathfrak{a}(\gamma) \sim \mathfrak{a}$. □

We now proceed to evaluate $\chi(\mathfrak{z})$ and $\chi(\mathfrak{w})$ in the various cases (a), (b), (c), using this lemma.

3. Results for even discriminants. First consider the case $d = -4p$, where $p \equiv 1 \pmod 8$. Here $q = 2$ and $\mathfrak{p} = (\sqrt{-p}) \sim 1$. Thus we need only compute $\chi(\mathfrak{w})$. We solve (4) with $a = 2$ by considering the prime factors of p in the field $Q(\sqrt{2})$. This field has class number 1, and so $(p) = \wp\wp'$ with

$$\wp = \left(u + w\sqrt{2}\right), \qquad w > 0, u^2 - 2w^2 = -p. \tag{5}$$

This solves (4) with $x = 2u$, $y = 1$, $z = w$, giving $\chi(\mathfrak{w}) = (w/p)$ by (1) and Lemma 1. (Note $p \nmid w$, so the Hilbert symbol $(w, d/p)$ equals the Legendre symbol (w/p).)

To characterize (w/p) in terms of a normal extension of Q we first note that $((w-u)/p) = 1$. For, by the law of quadratic reciprocity and the fact that $p \equiv 1 \pmod 8$ we have

$$\left(\frac{w-u}{p}\right) = \left(\frac{p}{w-u}\right) = \left(\frac{p - w^2 + u^2}{w-u}\right) = \left(\frac{w^2}{w-u}\right) = 1.$$

Hence

$$\left(\frac{w}{p}\right) = \left(\frac{(w-u)/w}{p}\right) = \left(\frac{1-u/w}{p}\right) = \left(\frac{1-u/w}{\wp}\right),$$

where the last symbol is the Legendre symbol in $Q(\sqrt{2})$. But from (5), $-u/w \equiv \sqrt{2} \pmod{\wp}$, so

$$\chi(\mathfrak{w}) = \left(\frac{1+\sqrt{2}}{\wp}\right).$$

In other words (see [**15**], p. 150), $\chi(\mathfrak{w}) = 1$ if and only if $\wp$ splits into 2 primes in the field $Q(\sqrt{\varepsilon})$, $\varepsilon = 1 + \sqrt{2}$. Note also that

$$\left(\frac{1+\sqrt{2}}{\wp'}\right) = \left(\frac{1-\sqrt{2}}{\wp}\right) = \left(\frac{-1}{\wp}\right)\left(\frac{1+\sqrt{2}}{\wp}\right) = \left(\frac{1+\sqrt{2}}{\wp}\right),$$

and so $\wp$ and $\wp'$ split the same way in $Q(\sqrt{\varepsilon})$. This field has the normal closure $K = Q(\sqrt{-1}, \sqrt{\varepsilon})$, which contains the 8th roots of unity. Hence we may state:

THEOREM 1. (*Cf.* [**1**].) *If p is an odd prime, then* 8 *divides the class number of $Q(\sqrt{-4p})$ if and only if p splits completely in the field* $K = Q(\sqrt{-1}\ \sqrt{1+\sqrt{2}}\ )$.

Since K is normal over Q of degree 8, the Frobenius density theorem ([**8**], II, p. 133) immediately gives the

COROLLARY. *The density of primes p for which* $8 \mid h(-4p)$ *is* $1/8$.

By similar methods one may also prove the following theorems. (Cf. [**12**], [**16**].)

THEOREM 2. (i) *If* $p \equiv 1 \pmod 8$, *then* $8 \mid h(-8p)$ *if and only if p splits completely in the field* $K' = Q(\sqrt{-1}, \sqrt[4]{2})$.

(ii) *If* $p \equiv -1 \pmod 8$, *then* $8 \mid h(-8p)$ *if and only if p splits completely in the* (*abelian*) *field* $K'' = Q(\sqrt{2+\sqrt{2}}\ )$, *i.e. if and only if* $p \equiv -1$ (mod 16).

(iii) *The density of p for which* $8 \mid h(-8p)$ *is* $1/4$.

THEOREM 3. *The restricted class number of* $Q(\sqrt{8p})$ *is divisible by* 8 *if and only if p splits completely in the field $K'K''$. The density of such primes is* $1/16$.

For the proof of Theorem 2 one starts with the formula $p = w^2 - 2u^2$, and shows that $(u/p) = 1$ in case (i) and $((w-u)/p) = (-p/(w-u)) = 1$ in case (ii). This leads as above to the characterization of $\chi(\mathfrak{w}) = (w/p)$ in terms of the fields K', K''. (Note here that $\mathfrak{p}\mathfrak{q} = (\sqrt{-2p}) \sim 1$, so $\chi(\mathfrak{w}) = \chi(\mathfrak{z})$.) We remark also that K'' is the subfield of the field of 16th roots of unity which corresponds in the sense of Galois theory to the group of automorphisms

$$H = \{(\zeta_{16} \to \zeta_{16}^a),\, a \equiv \pm 1 \pmod{16}\}, \qquad \zeta_{16} = e^{2\pi i/16}.$$

This follows from the formula

$$(\zeta_{16} + \zeta_{16}^{-1})^2 = 2 + \sqrt{2}.$$

Hence a prime $p \equiv -1 \pmod 8$ splits completely in K'' if and only if $p \equiv -1 \pmod{16}$. The density of p satisfying each of the respective conditions (i), (ii) is $1/8$, giving the total density $1/4$.

For Theorem 3 the evaluation of $\chi(\mathfrak{z})$ is accomplished using the formula

$$p = z^2 + 2y^2, \quad \text{where} \left(\frac{y}{p}\right) = +1,$$

while the evaluation of $\chi(\mathfrak{w})$ proceeds from

$$-p = w^2 - 2u^2$$

and the fact that $((w - u)/p) = +1$. We find that

$$\chi(\mathfrak{z}) = \left(\frac{\sqrt{2}}{\wp}\right), \qquad \chi(\mathfrak{w}) = \left(\frac{2 + \sqrt{2}}{\wp}\right), \tag{6}$$

where as before $(p) = \wp\wp'$ in $Q(\sqrt{2})$, and the symbols are Legendre symbols in $Q(\sqrt{2})$. We note $(\sqrt{2}/\wp) = (2/p)_4$, where $(a/p)_4 = \pm 1$ is the Dirichlet symbol, defined for quadratic residues a of p by $(a/p)_4 \equiv a^{(p-1)/4} \pmod p$.

Theorems 1–3 immediately imply the following curious result. (See **[16]**.)

THEOREM 4. *If p is a prime congruent to* $1 \pmod 8$, *then* $8 \mid h^+(8p)$ *if and only if* $8 \mid h(-4p)$ *and* $8 \mid h(-8p)$.

Proof. First note that $KK' = K'K''$ since

$$\sqrt[4]{2} \cdot \sqrt{1 + \sqrt{2}} = \sqrt{2 + \sqrt{2}}\,.$$

Thus p splits completely in $K'K''$ if and only if p splits completely in K and K'. □

While we are at it we also mention the following classical result, which follows easily from (6).

THEOREM 5. (*See* [4], *p*. 107.) *The Pell equation*

$$x^2 - 2py^2 = -1 \tag{7}$$

has a solution in integers if

$$p \equiv 9 \pmod{16} \quad \textit{and} \quad \left(\frac{2}{p}\right)_4 = -1. \tag{8}$$

If $p \equiv 1 \pmod 8$ *and exactly one* (*but not both*) *of the conditions in* (8) *holds, then* (7) *has no solution.*

Proof. In $\Omega = Q(\sqrt{2p})$ we have

$$\mathfrak{p}\mathfrak{q} = \left(\sqrt{2p}\right).$$

Thus $\mathfrak{p}\mathfrak{q} \sim 1$ if and only if some associate of $\sqrt{2p}$ has positive norm, which is the case exactly when the fundamental unit of $Q(\sqrt{2p})$ has norm -1. If either of the conditions in (8) holds then by (6) and the remarks following Theorem 3 we have $\chi(\mathfrak{z}) = -1$ or $\chi(\mathfrak{w}) = -1$, so that the 2-classgroup in Ω has order 4. Since $(\mathfrak{z}\mathfrak{w})^2 \sim \mathfrak{p}\mathfrak{q}$ it follows that $\mathfrak{p}\mathfrak{q} \sim 1$ if and only if $\chi(\mathfrak{z}\mathfrak{w}) = +1$, i.e. if and only if $\chi(\mathfrak{z}) = \chi(\mathfrak{w})$. This proves the theorem.

This concludes our discussion of cases (a) and (b). We turn now to case (c).

4. Results for odd discriminants.

For case (c) we require the following lemma.

LEMMA 2. *If* $\Delta \equiv 1 \pmod 4$ *and* $\gamma = (x + y\sqrt{\Delta})/2$ *is an integer of* $Q(\sqrt{\Delta})$ *which is relatively prime to* 2, *then* $\gamma^3 = u + v\sqrt{\Delta}$, *with* $u, v \in \mathbf{Z}$.

Proof. We may assume x and y are odd. Then the assumptions imply $\Delta \equiv 5 \pmod 8$, since

$$N\gamma = \frac{x^2 - \Delta y^2}{4} \equiv 0 \pmod 2$$

in case $\Delta \equiv 1 \pmod 8$. The assertion now follows easily by cubing and noting that $x^2 + 3\Delta y^2 \equiv 3x^2 + \Delta y^2 \equiv 0 \pmod 8$.

Consider first the computation of $\chi(\mathfrak{w})$, where $\mathfrak{w}^2 \sim \mathfrak{q}$. This entails solving (4) with $a = q$, i.e. solving

$$-p^* y^2 = 4z^2 - qx'^2, \qquad x = qx'. \tag{9}$$

For this we factor $(p) = \wp\wp'$ into conjugate prime ideals of degree 1 in $k = Q(\sqrt{q})$, which is possible since $(q/p) = +1$, and we consider the principal ideal $\wp^h$, where $h = h(q)$ is the class number of k. By Lemma 2 (with $\Delta = q$) we then have

$$(10) \qquad \wp^{3h} = \left(z' + x'\sqrt{q}\right), \qquad z', x' \in \mathbf{Z}, z' > 0.$$

Now the fundamental unit in k has norm -1, so on taking norms in (10) we may suppose that

$$(11) \qquad (-p^*)^{3h} = z'^2 - qx'^2.$$

Moreover h is odd (see **[9]**, p. 566), so that the lefthand side of (11) is $\equiv -1 \pmod 4$, implying that $2 \mid z'$; say $z' = 2z$. This solves (9) with $y = p^{(3h-1)/2}$.Thus by Lemma 1, (1) and (11) we see that

$$\begin{aligned}\chi(\mathfrak{w}) &= \left(\frac{z}{q}\right) = \left(\frac{2z'}{q}\right) = \left(\frac{2}{q}\right)\left(\frac{z'^2}{q}\right)_4 \\ &= \left(\frac{2}{q}\right)\left(\frac{-p^*}{q}\right)_4^{3h} = \left(\frac{p^*}{q}\right)_4,\end{aligned}$$

using the fact that h is odd, and noting $(2/p) = (-1/p)_4$.

This suffices for the computation of $\chi(\mathfrak{w})$. However, in order to characterize the primes p for which $\chi(\mathfrak{w}) = 1$ in terms of a normal extension of Q, we compute $\chi(\mathfrak{w})$ in a different way. Write $q = a^2 + b^2$, with $a, b \in \mathbf{Z}$, a odd, and assume for the moment that $p \nmid b$. Then $p \nmid (z' - ax')$, and we claim that $((z' - ax')/p) = 1$. For $z' - ax'$ is odd (and w.l.o.g. positive in case $p \equiv 3 \pmod 4$)), so by quadratic reciprocity (in the form given by Hasse **[9]**, p. 82) we have

$$\begin{aligned}\left(\frac{z' - ax'}{p}\right) &= \left(\frac{p^*}{z' - ax'}\right) = \left(\frac{(p^*)^{3h}}{z' - ax'}\right) \\ &= \left(\frac{(p^*)^{3h} + z'^2 - a^2x'^2}{z' - ax'}\right) = \left(\frac{b^2x'^2}{z' - ax'}\right) = 1.\end{aligned}$$

Therefore, by (1),

$$\begin{aligned}\chi(\mathfrak{w}) &= \left(\frac{z}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{z'}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{1 - a(x'/z')}{p}\right) \\ &= \left(\frac{2}{p}\right)\left(\frac{1 - a(x'/z')}{\wp}\right) \\ &= \left(\frac{\alpha}{\wp}\right),\end{aligned}$$

where $\alpha = (q + a\sqrt{q})/2$, using $-z'/x' \equiv \sqrt{q} \pmod{\wp}$ from (10). Hence $\chi(\mathfrak{w}) = 1$ if and only if $\wp$ splits completely in the field

$$K_q = Q\left(\sqrt{\frac{q + a\sqrt{q}}{2}}\right). \tag{12}$$

In case $p \mid b$ and $p \mid z' - ax'$, replace $z' - ax'$ in the above argument by $z' + ax'$. Then $p \nmid (z' + ax')$, since $p \nmid 2ax'$, and the computation shows that $\chi(\mathfrak{w}) = (\alpha'/\wp)$, where α' is the conjugate of α. Thus $\chi(\mathfrak{w}) = 1$ exactly when $\wp$ splits completely in $Q(\sqrt{\alpha'}) = Q(\sqrt{\alpha}) = K_q$, so we may drop the restriction $p \nmid b$.

Now the field K_q is abelian, because the conjugates of integer $\sqrt{\alpha}$ are $\pm\sqrt{\alpha}$, $\pm\sqrt{\alpha'} = \pm \frac{b}{2}\sqrt{q}\,\alpha^{-1}$, all of which lie in K_q, and because the substitution

$$\sqrt{\alpha} \to \sqrt{\alpha'}$$

is an automorphism of K_q of order 4. Consequently, $\wp$ splits completely in K_q if and only if the rational prime p does.

In particular, if $p \equiv 3 \pmod 4$, then $\Omega = Q(\sqrt{-pq})$ is imaginary, and

$$\mathfrak{p}\mathfrak{q} = \left(\sqrt{-pq}\right) \sim 1, \qquad \chi(\mathfrak{z}) = \chi(\mathfrak{w}).$$

Thus we have (cf. [**26**]):

THEOREM 6. *If $q \equiv 1 \pmod 4$ and $p \equiv 3 \pmod 4$, then $8 \mid h(-pq)$ if and only if p splits completely in the field K_q defined by* (12), *where $q = a^2 + b^2$, a odd. This is equivalent to the condition $(-p/q)_4 = 1$.*

COROLLARY 1. *For a fixed prime $q \equiv 1 \pmod 4$, the set of primes $p \equiv 3 \pmod 4$, for which $8 \mid h(-pq)$, has a density equal to $1/8$.*

Proof. This follows easily from Dirichlet's Theorem on primes in arithmetic progressions, since $1/4$ of the residue classes mod q satisfy

$$a^{(q-1)/4} \equiv (-1)^{(q-1)/4} \pmod{q}.$$

COROLLARY 2. *For a fixed $p \equiv 3 \pmod 4$, the set of primes $q \equiv 1 \pmod 4$, for which $8 \mid h(-pq)$, has density $1/8$.*

Proof. For fixed p, $(-p/q)_4 = 1$ if and only if q splits completely in $L = Q(\sqrt{-1}, \sqrt[4]{-p})$, which has degree 8 over Q. The corollary now follows from the Frobenius density theorem.

We mention several special cases of Theorem 6 in

COROLLARY 3. *If p is a prime* $\equiv 3 \pmod 4$, *then*
(i) $8 \mid h(-5p)$ *if and only if* $p \equiv 19 \pmod{20}$,
(ii) $8 \mid h(-13p)$ *if and only if* $p \equiv 23, 43, 51 \pmod{52}$,
(iii) $8 \mid h(-17p)$ *if and only if* $p \equiv 35, 47, 55, 67 \pmod{68}$.

In the final case $p \equiv 1 \pmod 4$, the field $\Omega = Q(\sqrt{pq})$ is real, and p and q enter symmetrically. We conclude immediately that

$$(13) \qquad \chi(\mathfrak{z}) = \left(\frac{q}{p}\right)_4, \qquad \chi(\mathfrak{w}) = \left(\frac{p}{q}\right)_4 = \left(\frac{\alpha}{\wp}\right).$$

Thus we have (cf. [**26**]):

THEOREM 7. *For primes $p, q \equiv 1 \pmod 4$, $8 \mid h^+(pq)$ if and only if p splits completely in the field*

$$\Lambda_q = K_q \cdot Q\left(\sqrt{-1}, \sqrt[4]{q}\right),$$

which has degree 16 *over* Q. *The density of such primes is* $1/16$.

Related to Theorem 7 is the following result on the Pell equation

$$(14) \qquad x^2 - pqy^2 = -1,$$

which is proved from (13) by the same argument used to prove Theorem 5.

THEOREM 8. *Let* p, q *be distinct primes* $\equiv 1 \pmod 4$, *for which* $(p/q) = 1$. *If* $(p/q)_4 = (q/p)_4 = -1$, *then equation* (14) *has a solution in integers. If* $(p/q)_4 \neq (q/p)_4$, *then* (14) *has no solution.*

As a corollary of our discussion we see that an odd prime $p \neq q$ splits completely in K_q if and only if $(p^*/q)_4 = 1$. In the language of classfield theory this says that K_q is the classfield over Q corresponding to the rational ideal group

$$H_q = \left\{u \in Q: u > 0, (u, 2q) = 1, \left(\frac{u}{q}\right) = \psi(u) = 1\right\},$$

where ψ is one of the two conjugate quartic characters modulo $4q$ defined on quadratic residues of q by $\psi(u) = (u^*/q)_4$. This character has conductor $f = q$ or $4q$ according as $q \equiv 1$ or $5 \pmod 8$. The correspondence of K_q

to H_q may also be deduced using the "rational" Gaussian sum

$$\tau'(\psi) = \sum_{\substack{u \,(\mathrm{mod}\, f)\\ \psi(u) = \pm 1}} \psi(u)\zeta_f^u,$$

which has the value $\pm\sqrt{(q - a\sqrt{q})/2}$ if $q \equiv 1 \pmod 8$ and $\pm 2\sqrt{(q + a\sqrt{q})/2}$ if $q \equiv 5 \pmod 8$, where $q = a^2 + b^2$, $a \equiv 1 \pmod 4$. We omit the proof, which proceeds by rearranging the real and imaginary parts of the usual Gaussian sum

$$\tau(\psi_1) = \sum_{u \,(\mathrm{mod}\, q)} \psi_1(u)\zeta_q^u$$

corresponding to the character $\psi_1(u) = (u/q)_4$. (See also Hasse [**10**], p. 492.)

We note in addition that the second equation in (13) is equivalent to a result of E. Lehmer ([**19**], Theorem 2), according to which

$$\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = \left(\frac{\alpha_1}{\wp}\right), \qquad (p \equiv q \equiv 1 \pmod 4)$$

where $\alpha_1 = (a + \sqrt{q})/2$ and the sign of a is chosen so that $\wp \nmid \alpha_1$. This has been derived as a consequence of the arithmetic in the fields $\Omega = Q(\sqrt{pq})$ and $k = Q(\sqrt{q})$, quadratic reciprocity, and equation (1), which is itself a consequence of the product formula for the Hilbert symbol.

References

[1] P. Barrucand and H. Cohn, *Note on primes of type $x^2 + 32y^2$, class number and residuacity*, J. Reine Angew. Math., **238** (1969), 67–70.

[2] H. Bauer, *Die 2-Klassenzahlen spezieller quadratischer Zahlkörper*, J. Reine Angew. Math., **252** (1972), 79–81.

[3] E. Brown, *Class numbers of quadratic fields*, Symposia Math., **XV** (1975), 403–411.

[4] H. Cohn, *A Classical Invitation to Algebraic Numbers and Classfields*, New York, 1978.

[5] H. Cohn and J. C. Lagarias, *Is there a density for the set of primes p such that the class number of $Q(\sqrt{-p})$ is divisible by* 16?, to appear.

[6] ______, *On the existence of fields governing the* 2*-classgroup of $Q(\sqrt{dp})$ as p varies*, to appear.

[7] D. Estes and G. Pall, *Spinor genera of binary quadratic forms*, J. Number Theory, **5** (1973), 421–432.

[8] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper I, Ia, II*, Würzburg, 1970.

[9] ______, *Zahlentheorie*, Berlin, 1969.

[10] ______, *Vorlesungen über Zahlentheorie*, Berlin, 1964.

[11] ______, *Über die Klassenzahl des Körpers $P(\sqrt{-p})$ mit einer Primzahl $p \equiv 1 \bmod 2^3$*, Aequationes Math., **3** (1969), 254–258.

[12] ______, *Über die Klassenzahl des Körpers $P(\sqrt{-2p})$ mit einer Primzahl $p \neq 2$*, J. Number Theory, **1** (1969), 231–234.

[13] _____, *Über die Teilbarkeit durch* 2^3 *der Klassenzahl quadratischer Zahlkörper mit genau zwei verschiedenen Diskriminantenprimteilern*, Math. Nachr., **46** (1970), 61–70.
[14] _____, *An algorithm for determining the structure of the 2-Sylow subgroup of the divisor class group of a quadratic number field*, Symposia Math., **XV** (1975), 341–352.
[15] E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, New York, 1970.
[16] P. Kaplan, *Divisibilité par 8 du nombre des classes des corps quadratiques dont le 2-groupe de classes est cyclique et réciprocité biquadratique*, J. Math. Soc. Japan, **25** (1973), 596–608.
[17] _____, *Cycles d'ordre au moins 16 dans le 2-groupe des classes d'ideaux de certains corps quadratiques*, Calculateurs en Math. (1975-Limoges), Bull. Soc. Math. France, Mémoire, **49–50** (1977), 113–124.
[18] P. Kaplan and C. Sanchez, *Table de 2-groupes d'ideaux au sens restreint et des facteurs principaux des corps quadratiques réels* $Q(\sqrt{2p})$, $p < 2{,}000{,}000$, Université de Nancy I, U.E.R. de Mathematique, 1975.
[19] E. Lehmer, *On the quadratic character of some quadratic surds*, J. Reine Angew. Math., **250** (1971), 42–48.
[20] P. Morton, *On Rédei's theory of the Pell equation*, J. Reine Angew. Math., **307/308** (1979), 373–398.
[21] _____, *Density results for the 2-classgroups of imaginary quadratic fields*, J. Reine Angew. Math., **332** (1982), 156–187.
[22] _____, *Density results for the 2-classgroups and fundamental units of real quadratic fields*, to appear in Studia Scientiarum Mathematicarum Hungarica.
[23] B. Oriat, *Relations entre les 2-groupes de classes d'ideaux des extensions quadratiques* $k(\sqrt{d})$ *et* $k(\sqrt{-d})$, Ann. Inst. Fourier, Grenoble, **27**, 2 (1977), 37–59.
[24] _____, *Sur la divisibilité par 8 et 16 des nombres de classes d'ideaux des corps quadratiques* $Q(\sqrt{2p})$ *et* $Q(\sqrt{-2p})$, J. Math. Soc. Japan, **30**, 2 (1978), 279–285.
[25] L. Rédei, *Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper*, J. Reine Angew. Math., **171** (1934), 55–60.
[26] _____, *Über die Grundeinheit und die durch 8 teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper*, J. Reine Angew. Math., **171** (1934), 131–148.
[27] _____, *Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper*, J. Reine Angew. Math., **180** (1938), 1–43.
[28] _____, *Die Diophantische Gleichung* $mx^2 + ny^2 = z^4$, Monatshefte Math., **48** (1939), 43–60.
[29] H. Reichardt, *Über die 2-Klassengruppe gewisser quadratischer Zahlkörper*, Math. Nachr., **46** (1970), 71–80.
[30] W. C. Waterhouse, *Pieces of eight in class groups of quadratic fields*, J. Number Theory, **5** (1973), 95–97.

Received November 6, 1981 and in revised form April 28, 1982. The contents of this paper are taken from the author's doctoral dissertation, given at the University of Michigan, 1979.

HARVARD UNIVERSITY
CAMBRIDGE, MA 02138