ON THE DIVISIBILITY OF THE CLASS NUMBER OF $\mathbb{Q}(\sqrt{-pq})$ BY 16

by PHILIP A. LEONARD and KENNETH S. WILLIAMS*

(Received 29th January 1982)

1. Introduction

Let $d(<0)$ denote a squarefree integer. The ideal class group of the imaginary quadratic field $\mathbb{Q}(\sqrt{d})$ has a cyclic 2-Sylow subgroup of order $\geq 8$ in precisely the following cases (see for example [5] and [6]):

(i) $d = -p$, $p = 2g^2 - h^2 \equiv 1 \pmod{8}$, $(g/p) = +1$;
(ii) $d = -2p$, $p = u^2 - 2v^2 \equiv 1 \pmod{8}$ with $u$ chosen so that $u \equiv 1 \pmod{4}$, $(u/p) = +1$;
(iii) $d = -2p$, $p \equiv 15 \pmod{16}$;
(iv) $d = -pq$, $p \equiv 1 \pmod{4}$, $q \equiv 3 \pmod{4}$, $(q/p) = +1$, $(-q/p)_4 = +1$,

where $p$ and $q$ denote primes and $g$, $h$, $u$ and $v$ are positive integers. The class number of $\mathbb{Q}(\sqrt{d})$ is denoted by $h(d)$ and in the above cases $h(d) \equiv 0 \pmod{8}$. For cases (i), (ii) and (iii) the authors [6] have given necessary and sufficient conditions for $h(d)$ to be divisible by 16. In this paper we do the same for case (iv) extending the results of Brown [4].

As the ideal class group of $\mathbb{Q}(\sqrt{-pq})$ is isomorphic to the group (under composition) of classes of integral positive-definite binary quadratic forms $(a, b, c) = ax^2 + bxy + cy^2$ of discriminant $b^2 - 4ac = -pq$, we can work with forms rather than ideals. In order to determine $h(-pq)$ modulo 16 we construct explicitly a form $f$ of discriminant $-pq$ whose square is in the ambiguous class containing the form $(p, p, \frac{1}{2}(p+q))$ (see Theorem 1 in Section 2). The form $f$ is given in terms of a solution in positive integers $X, Y, Z$ of the Legendre equation

$$pX^2 + qY^2 - Z^2 = 0$$

satisfying

$$(X, Y) = (Y, Z) = (Z, X) = 1, \ p \nmid YZ, \ q \nmid XZ,$$

and

$$X \ odd, \ Y \ even, \ Z \equiv 1 \pmod{4}.$$  

*Research supported by Natural Sciences and Engineering Research Council Canada Grant No. A-7233 and also by a travel grant from Carleton University.
That there is a solution of (1.1) satisfying (1.2) follows immediately from Legendre's theorem in view of (iv). However we must justify that we can always find a solution with \( Z \equiv 1 \pmod{4} \). In order to see this we let \( R + S \sqrt{q} \) be the fundamental unit \((>1)\) of the real quadratic field \( \mathbb{Q}(\sqrt{q}) \). As \( q \equiv 3 \pmod{4} \) we have
\[
R^2 - qS^2 = +1.
\]
It is well known that
\[
R \equiv 2 \pmod{8}, \quad S \equiv 1 \pmod{2}, \quad \text{if} \quad q \equiv 3 \pmod{8},
\]
\[
R \equiv 0 \pmod{8}, \quad S \equiv 1 \pmod{2}, \quad \text{if} \quad q \equiv 7 \pmod{8},
\]
and hence
\[
R_1 = R^2 + qS^2 \equiv 7 \pmod{8}, \quad S_1 = 2RS \equiv 0 \pmod{4}, \quad R_1^2 - qS_1^2 = +1.
\]
Hence if \( Z \) is even (so that \( X \) and \( Y \) are both odd) we can replace the solution \((X, Y, Z)\) of (1.1) by the solution \((X_1, Y_1, Z_1)\) given by
\[
X_1 = X, \quad Y_1 = RY + SZ, \quad Z_1 = qSY + RZ,
\]
for which \( Z_1 \) is odd. Further if \( Z \equiv 3 \pmod{4} \) (in which case \( X \) is odd and \( Y \) is even) we can replace the solution \((X, Y, Z)\) by the solution \((X_2, Y_2, Z_2)\) given by
\[
X_2 = X, \quad Y_2 = R_1 Y + S_1 Z, \quad Z_2 = qS_1 Y + R_1 Z,
\]
for which \( Z_2 \equiv 1 \pmod{4} \).

Our main result is the following theorem.

**Theorem 2.** If \( p \) and \( q \) are primes such that
\[
p \equiv 1 \pmod{4}, \quad q \equiv 3 \pmod{4}, \quad \left( \frac{p}{q} \right) = +1, \quad \left( \frac{-q}{p} \right) = +1,
\]
and \((X, Y, Z)\) is any solution in positive integers of (1.1) which satisfies (1.2) and (1.3), then
\[
h(-pq) \equiv 0 \pmod{16} \Rightarrow \left( \frac{Z}{p} \right)_4 = \left( \frac{2X}{Z} \right)_4.
\]

We remark that \((Z/p)_4\) is well-defined as \((Z/p) = +1\) and \( p \equiv 1 \pmod{4} \). To see that \((Z/p) = +1\) we perform the following calculation: letting \( Y = 2^n Y_1, \ Y_1 \) odd, we have, using
ON THE DIVISIBILITY OF THE CLASS NUMBER OF \( Q(\sqrt{-pq}) \) BY 16

(1.1) and (1.2),

\[
\left( \frac{Z}{p} \right) = \left( \frac{Z^2}{p} \right) = \left( \frac{qY^2}{p} \right) = \left( \frac{q}{p} \right) \left( \frac{Y}{p} \right) = \left( \frac{q}{p} \right) \left( \frac{2}{p} \right)^n \left( \frac{Y_1}{p} \right)
\]

\[
= \left( \frac{q}{p} \right) \left( \frac{2}{p} \right) \left( \frac{p}{Y_1} \right) \quad (\text{as } n = 1 \text{ when } p \equiv 5 \pmod{8})
\]

\[
= \left( \frac{q}{p} \right) \left( \frac{-1}{p} \right) \left( \frac{pX^2}{Y_1} \right) \quad (\text{as } p \equiv 1 \pmod{4})
\]

\[
= \left( \frac{-q}{p} \right) \left( \frac{Z^2}{Y_1} \right)
\]

\[
= +1. \quad \text{(by (1.4)).}
\]

2. Square root of \((p, p, (p+q)/4)\)

In this section we construct a form \( f \) of discriminant \(-pq\) such that \( f^2 \sim (p, p, \frac{1}{4}(p+q)) \).

As \((X, Y) = 1\) there exists an integer \( u_0 \) such that \( u_0X \equiv 1 \pmod{Y} \). If the integer \( e = (u_0X - 1)/Y \) is odd we set \( u = u_0 \). If the integer \( (u_0X - 1)/Y \) is even then the integer

\[
e = (u_0 + Y)X - 1 \equiv u_0X - 1 \equiv X \pmod{Y}
\]

is odd and we set \( u = u_0 + Y \). Thus the integers \( u \) and \( e \) satisfy

\[
uX \equiv 1 \pmod{Y}, \ u \text{ odd, } e = (uX - 1)/Y \text{ odd.} \quad (2.1)
\]

Next, appealing to (1.1) and (2.1), we have

\[
X(pX - uZ^2) \equiv 0 \pmod{Y}
\]

so that, as \((X, Y) = 1\), we have

\[
pX - uZ^2 \equiv 0 \pmod{Y}.
\]

Hence we can define a positive integer \( a \) and an integer \( b \) by

\[
a = Z, \ b = (pX - u^2)/Y. \quad (2.2)
\]

From (2.2) we obtain

\[
pX - bY = u^2. \quad (2.3)
\]
Also using (1.1), (2.1) and (2.2) we get
\[ bX + qY = -ea^2, \]  
(2.4)
and
\[ b^2 + pq = (pe^2 + qu^2)a^2. \]  
(2.5)

From (1.4) and (2.1) we see that \( pe^2 + qu^2 \equiv 0 \pmod{4} \) so we can define an integer \( c \) by
\[ c = (pe^2 + qu^2)/4. \]  
(2.6)
Thus, from (2.5) and (2.6), we have
\[ b^2 - 4a^2c = -pq, \]  
(2.7)
showing that the form \( (a,b,ac) \) has discriminant \(-pq\). We note that (2.7) shows that \( b \) is odd.

With \( a, b \) and \( c \) as defined in (2.2) and (2.6) we prove the following theorem.

**Theorem 1.** \( (a,b,ac)^2 \sim (p,p,(p+q)/4). \)

**Proof.** We define integers \( v, \alpha \) and \( \beta \) by
\[ v = 2Y, \quad \alpha = (u+e)/2, \quad \beta = X + Y. \]  
(2.8)
Appealing to (1.1), (2.3) and (2.7) we obtain, on completing the square for \( u, \)
\[ a^2u^2 + buv + cv^2 = p, \]  
(2.9)
and appealing to (2.3), (2.4), (2.7) and (2.8), we obtain
\begin{align*}
bu + 2cv &= \frac{1}{a^2} (bua^2 + 4a^2cY) \\
&= \frac{1}{a^2} (bua^2 + (b^2 + pq)Y) \\
&= \frac{1}{a^2} (b(bY + ua^2) + pqY) \\
&= \frac{1}{a^2} (bpX + pqY),
\end{align*}
ON THE DIVISIBILITY OF THE CLASS NUMBER OF $Q(\sqrt{-pq})$ BY 16

that is

$$bu + 2cv = -pe. \quad (2.10)$$

Hence from (2.3), (2.8) and (2.10) we have

$$\alpha = (pu - bu - 2cv)/2p, \quad \beta = (2ua^2 + bv + pv)/2p. \quad (2.11)$$

Thus from (2.9) and (2.11) we obtain

$$u\beta - v\alpha = 1 \quad (2.12)$$

and

$$2a^2ux + bu\beta + bvx + 2cv\beta = p. \quad (2.13)$$

Hence from (2.7), (2.9) (2.12) and (2.13) and the identity

$$(2a^2ux + bu\beta + bvx + 2cv\beta)^2 - 4(a^2u^2 + buv + cv^2)(a^2x^2 + b\alpha\beta + c\beta^2) = (u\beta - v\alpha)^2(b^2 - 4a^2c),$$

we deduce

$$a^2x^2 + b\alpha\beta + c\beta^2 = (p + q)/4. \quad (2.14)$$

Hence the unimodular transformation with matrix $\begin{bmatrix} u & v \\ \beta & \gamma \end{bmatrix}$ changes the form $(a^2, b, c)$ into

$$(a^2u^2 + buv + cv^2, 2a^2ux + bu\beta + bvx + 2cv\beta, a^2x^2 + b\alpha\beta + c\beta^2) = (p, p, (p + q)/4).$$

Thus we have (see for example [3, p. 185])

$$(a, b, ac)^2 \sim (a^2, b, c) \sim (p, p, (p + q)/4),$$

which completes the proof of Theorem 1.

3. Determination of $h(-pq)$ modulo 16; Proof of Theorem 2

By Theorem 1 the class of the form $(a, b, ac)$ is of order 4 and so as the 2-Sylow subgroup of the class group of forms of discriminant $-pq$ is cyclic, the form $(a, b, ac)$ is equivalent to the square of a form $(r, s, t)$, where we may take $(r, 2pqac) = 1$. Hence $(a, b, ac)$ represents $r^2$ primitively so that there are integers $x$ and $y$ such that

$$r^2 = ax^2 + bxy + acy^2, \quad x > 0, \quad (x, y) = 1. \quad (3.1)$$

We define non-negative integers $S$ and $T$ by

$$S = |2Xx - aey|, \quad T = |2Yx - axy|. \quad (3.2)$$
Appealing to (1.1), (2.1), (2.2), (2.6) and (3.1) we obtain
\[ 4ar^2 = pS^2 + qT^2. \] (3.3)

From (3.3) we easily deduce that \( S \) and \( T \) are positive.

We now show that \( S \) and \( T \) have no odd common divisors greater than 1. Suppose \( k \) is an odd prime divisor of both \( S \) and \( T \). Then \( k \) divides
\[ u(2Xx - aey) - e(2Yx - auy) \]
\[ = 2x(uX - eY) \]
\[ = 2x \quad \text{(by (2.1)),} \]
that is \( k|x \). Further from (3.3) we have \( k|ar^2 \) so that \( k|a \) or \( k|r \). If \( k|a \) from (3.1) we have \( k|r \) contradicting \( (r, a) = 1 \). If \( k|r \) by (3.1) we have \( k|acy^2 \) contradicting \( (r, ac) = (x, y) = 1 \).

Similarly we can show that \( T \) and \( apr \) have no odd common divisors greater than 1.

We note that as \( a \) is represented by \( (a, b, ac) \) and the class of the form \( (a, b, ac) \) is in the principal genus we have
\[ \left( \frac{a}{p} \right) = +1. \] (3.4)

Further by (1.3) and (2.2) we have
\[ a \equiv 1 \pmod{4}. \] (3.5)

Then
\[ \left( \frac{r}{p} \right) \left( \frac{a}{p} \right)_4 = \left( \frac{ar^2}{p} \right)_4 = \left( \frac{2}{p} \right) \left( \frac{4ar^2}{p} \right)_4 \]
\[ = \left( \frac{-1}{p} \right)_4 \left( \frac{qT^2}{p} \right)_4 \quad \text{(by (3.3))} \]
\[ = \left( \frac{-q}{p} \right)_4 \left( \frac{T}{p} \right)_4. \]

that is (by (1.4))
\[ \left( \frac{r}{p} \right) \left( \frac{a}{p} \right)_4 = \left( \frac{T}{p} \right)_4 = \left( \frac{2}{p} \right)^n \left( \frac{t}{p} \right). \] (3.6)

where
\[ T = 2^t, \quad t \text{ odd.} \] (3.7)
ON THE DIVISIBILITY OF THE CLASS NUMBER OF $Q(\sqrt{-pq})$ BY 16

Then

$$\left(\frac{t}{p}\right) = \left(\frac{p}{t}\right)$$

$$= \left(\frac{ps^2}{t}\right)$$

$$= \left(\frac{4ar^2}{t}\right) \quad \text{(by (3.3))}$$

$$= \left(\frac{a}{t}\right)$$

$$= \left(\frac{t}{a}\right) \quad \text{(by (3.5))}$$

$$= \left(\frac{2}{a}\right)^* \left(\frac{T}{a}\right) \quad \text{(by (3.7))}$$

$$= \left(\frac{2}{a}\right)^* \left(\frac{2Yx - auy}{a}\right)$$

$$= \left(\frac{2}{a}\right)^* \left(\frac{2Yx - auy}{a}\right) \quad \text{(by (3.5))}$$

$$= \left(\frac{2}{a}\right)^{n+1} \left(\frac{Y}{a}\right) \left(\frac{x}{a}\right)$$

$$= \left(\frac{2}{a}\right)^{n+1} \left(\frac{Y}{a}\right) \left(\frac{b}{a}\right) \left(\frac{y}{a}\right) \quad \text{(by (3.1)).}$$

Now set

$$|y| = 2^m y_1, \quad y_1 \text{ odd, } \quad y_1 > 0,$$

so appealing to (3.1) and (3.5) we have

$$\left(\frac{y}{a}\right) = \left(\frac{|y|}{a}\right) = \left(\frac{2}{a}\right)^m \left(\frac{y_1}{a}\right) = \left(\frac{2}{a}\right)^m \left(\frac{a}{y_1}\right) = \left(\frac{2}{a}\right)^m,$$

giving

$$\left(\frac{t}{p}\right) = \left(\frac{2}{a}\right)^{m+n+1} \left(\frac{bY}{a}\right).$$
Next as $bY = pX - ua^2$ and using (3.4) we have

$$\left( \frac{bY}{a} \right) = \left( \frac{pX}{a} \right) = \left( \frac{a}{p} \right) \left( \frac{X}{Z} \right) = \left( \frac{X}{Z} \right),$$

so

$$\left( \frac{t}{p} \right) = \left( \frac{X}{Z} \right)^{m+n+1},$$

giving

$$\left( \frac{r}{p} \right) = \left( \frac{2}{p} \right)^n \left( \frac{2}{Z} \right)^{m+n+1} \left( \frac{X}{Z} \right) \left( \frac{a}{p} \right)_4.$$  \hfill (3.8)

Taking (1.1) modulo 8 we obtain $p + qY^2 \equiv 1 \pmod{8}$, so that

- $p \equiv 1 \pmod{8} \Rightarrow Y \equiv 0 \pmod{4},$
- $p \equiv 5 \pmod{8} \Rightarrow Y \equiv 2 \pmod{4}.$

We now treat the case $p \equiv 1 \pmod{8}$: we have

- $m = 0 \Rightarrow y \text{ odd} \Rightarrow T \text{ odd} \Rightarrow n = 0;$
- $m = 1 \Rightarrow 2 \mid y \Rightarrow 2 \mid T \Rightarrow n = 1;$
- $m = 2 \Rightarrow 4 \mid y \Rightarrow 4 \mid T \Rightarrow n = 2;$
- $m \geq 3 \Rightarrow 8 \mid y \Rightarrow x \text{ odd} \Rightarrow a \equiv 1 \pmod{8} \Rightarrow \left( \frac{2}{Z} \right) = +1;$

so that in each case

$$\left( \frac{2}{p} \right)^n \left( \frac{2}{Z} \right)^{m+n} = 1.$$

For the case $p \equiv 5 \pmod{8}$ we have

- $m = 0 \Rightarrow y \text{ odd} \Rightarrow T \text{ odd} \Rightarrow n = 0;$
- $m = 1 \Rightarrow 2 \mid y \Rightarrow 4 \mid S, 2 \mid T \Rightarrow pS^2 + qT^2 \equiv 12 \pmod{16}$
  \Rightarrow ar^2 \equiv 3 \pmod{4}, \text{ which is impossible;}
- $m = 2 \Rightarrow x \text{ odd}, 4 \mid y \Rightarrow a \equiv 5 \pmod{8} \Rightarrow \left( \frac{2}{Z} \right) = -1;$
ON THE DIVISIBILITY OF THE CLASS NUMBER OF \( Q(\sqrt{-pq}) \) BY 16

\[ m \geq 3 \Rightarrow x \text{ odd}, \quad 8 | y \Rightarrow \begin{cases} a \equiv 1 \pmod{8} \Rightarrow \left( \frac{2}{Z} \right) = +1, \\ 4 \mid T \Rightarrow n = 2; \end{cases} \]

so that again in each case we have

\[ \left( \frac{2}{p} \right) \left( \frac{2}{Z} \right)^{m+n} = 1. \]

Hence by (3.8) we have

\[ \left( \frac{r}{p} \right) = \left( \frac{2}{Z} \right) \left( \frac{X}{Z} \right) \left( \frac{1}{p} \right)_4. \]

Now by a theorem of Bauer [1] (see also [2, Theorem 6])

\[ h(-pq) \equiv 0 \pmod{16} \Leftrightarrow \left( \frac{r}{p} \right) = +1 \]

so we have

\[ h(-pq) \equiv 0 \pmod{16} \Leftrightarrow \left( \frac{Z}{p} \right)_4 = \left( \frac{2X}{Z} \right). \]

This completes the proof of Theorem 2.

We remark that Theorem 2 of Brown [4] is the special case of our Theorem 2 which arises when (1.1) has a solution with \( X = 1 \).

4. Examples

Example 1. \( p = 5, \quad q = 19 \).

Here

\[ \left( \frac{q}{p} \right) = \left( \frac{19}{5} \right) = 1, \quad \left( \frac{-q}{p} \right)_4 = \left( \frac{-19}{5} \right)_4 = +1. \]

A solution of (1.1)-(1.3) is given by

\[ X = 1, \quad Y = 2, \quad Z = 9 \]

so

\[ \left( \frac{Z}{p} \right)_4 = \left( \frac{9}{5} \right)_4 = \left( \frac{3}{5} \right) = -1, \quad \left( \frac{2X}{Z} \right) \left( \frac{2}{9} \right) = +1, \]
and Theorem 2 implies $h(-pq) = h(-95) \equiv 8 \pmod{16}$. Indeed $h(-95) = 8$.

**Example 2.** $p = 37$, $q = 11$.

Here

$$\left( \frac{q}{p} \right) = \left( \frac{11}{37} \right) = \left( \frac{37}{11} \right) = \left( \frac{4}{11} \right) = +1, \quad \left( \frac{-q}{p} \right)_4 = \left( \frac{-11}{37} \right)_4 = \left( \frac{100}{37} \right)_4 = \left( \frac{10}{37} \right) = +1.$$

We start with a solution of (1.1) and (1.2) for which $Z$ is even, say,

$$X = 1, \quad Y = 7, \quad Z = 24,$$

in order to illustrate how to obtain a solution which satisfies (1.3) as well. Since the fundamental unit of $Q(\sqrt{11})$ is $10 + 3\sqrt{11}$ we have

$$R = 10, \quad S = 3, \quad R_1 = 199, \quad S_1 = 60.$$

First we transform the solution $(X, Y, Z)$ into a solution $(X_1, Y_1, Z_1)$ with $Z_1$ odd:

$$X_1 = X = 1, \quad Y_1 = RY + SZ = 142, \quad Z_1 = qSY + RZ = 471.$$

As $Z_1 \equiv 3 \pmod{4}$ we transform the solution $(X_1, Y_1, Z_1)$ into a solution $(X_2, Y_2, Z_2)$ with $Z_2 \equiv 1 \pmod{4}$:

$$X_2 = X_1 = 1, \quad Y_2 = R_1Y_1 + S_1Z_1 = 56518, \quad Z_2 = qS_1Y_1 + R_1Z_1 = 187449,$$

so that

$$\left( \frac{Z_2}{p} \right)_4 = \left( \frac{187449}{37} \right)_4 = \left( \frac{7}{37} \right)_4 = \left( \frac{81}{37} \right)_4 = +1, \quad \left( \frac{2X_2}{Z_2} \right)_4 = \left( \frac{2}{187449} \right)_4 = +1,$$

and Theorem 2 implies $h(-pq) = h(-407) \equiv 0 \pmod{16}$. Indeed $h(-407) = 16$.

**Example 3.** $p = 5$, $q = 79$.

Here

$$\left( \frac{q}{p} \right) = \left( \frac{79}{5} \right) = +1, \quad \left( \frac{-q}{p} \right)_4 = \left( \frac{-79}{5} \right)_4 = +1.$$

A solution of (1.1) and (1.2) is given by

$$X = 3, \quad Y = 2, \quad Z = 19.$$
ON THE DIVISIBILITY OF THE CLASS NUMBER OF $Q(\sqrt{-pq})$ BY 16

As $Z \equiv 3(\mod 4)$ we transform this solution into one for which $Z \equiv 1(\mod 4)$ obtaining

$$X = 3, \quad Y = 52958, \quad Z = 470701,$$

so that

$$\left(\frac{Z}{p}\right)_4 = +1, \quad \left(\frac{2X}{Z}\right) = \left(\frac{2}{Z}\right) = (-1)(+1) = -1,$$

and Theorem 2 implies $h(-pq) = h(-395) \equiv 8(\mod 16)$. Indeed $h(-395) = 8$.

This example illustrates Theorem 2 in a situation where (1.1) has no solution with $X = 1$ as

$$u^2 - 79v^2 = 5$$

is insolvable in integers $u$ and $v$ (see for example [7, Theorem 109]).

REFERENCES


2. Ezra Brown, The power of 2 dividing the class-number of a binary quadratic discriminant, J. Number Theory 5 (1973), 413–419.


4. Ezra Brown, The class-number of $Q(\sqrt{-pq})$, for $p \equiv -q \equiv 1(\mod 4)$ primes, Houston J. Math. 7 (1981), 497–505.


Department of Mathematics
Arizona State University
Tempe, Arizona 85287, U.S.A.

Department of Mathematics
and Statistics
Carleton University
Ottawa, Ontario, Canada K1S 5B6