Canad. Math. Bull. Vol. **25** (2), 1982

ON THE DIVISIBILITY OF THE CLASS NUMBERS OF $Q(\sqrt{-p})$ AND $Q(\sqrt{-2p})$ BY 16.

BY

PHILIP A. LEONARD AND KENNETH S. WILLIAMS*

ABSTRACT. Let $h(m)$ denote the class number of the quadratic field $Q(\sqrt{m})$. In this paper necessary and sufficient conditions for $h(m)$ to be divisible by 16 are determined when $m=-p$, where p is a prime congruent to 1 modulo 8, and when $m=-2p$, where p is a prime congruent to ± 1 modulo 8.

0. **Introduction.** Let $D=-p$, where p is a prime congruent to 1 modulo 8, or $D=-2p$, where p is a prime congruent to ± 1 modulo 8. Let $h(D)$ denote the class number of the imaginary quadratic field $Q(\sqrt{D})$. For these values of D, the 2-Sylow subgroup $H_2(D)$ of the class group $H(D)$ of $Q(\sqrt{D})$ is cyclic of order ≥ 4, so that $h(D) \equiv 0 \pmod 4$. Moreover, in each of these cases, necessary and sufficient conditions for $h(D)$ to be divisible by 8 are known in terms of congruences involving the positive integers u and v in the representation

$$p=u^2-2v^2. \tag{0.1}$$

In this paper, using the fact that $H_2(D)$ is cyclic, we determine the corresponding criteria for $h(D)$ to be divisible by 16.

1. $D=-p$, $p\equiv 1 \pmod 8$. We set $g=u+v$, $h=u+2v$ so that g and h are odd positive integers satisfying

$$p=2g^2-h^2. \tag{1.1}$$

Clearly we have

$$\text{G.C.D.}\,(g,p)=\text{G.C.D.}\,(h,p)=\text{G.C.D.}\,(g,h)=1. \tag{1.2}$$

Brown [3: Theorem 2] has shown that

$$h(-p)\equiv 0 \pmod 8 \Leftrightarrow \left(\frac{g}{p}\right)=+1, \tag{1.3}$$

Received by the editors May 2, 1980.
AMS (1980) classification numbers: 12A25, 12A50.
Key words and phrases: class number, imaginary quadratic field, binary quadratic forms.

* Research supported by the Natural Sciences and Engineering Research Council of Canada under grant A-7233.

and Hasse [6: p. 168] has shown that

$$h(-p) \equiv 0 (\text{mod } 8) \Leftrightarrow g \equiv 1 (\text{mod } 4). \tag{1.4}$$

It is easy to see that (1.3) and (1.4) are equivalent since, by appealing to (1.1) and the law of quadratic reciprocity, we have

$$\left(\frac{g}{p}\right) = \left(\frac{p}{g}\right) = \left(\frac{2g^2 - h^2}{g}\right) = \left(\frac{-h^2}{g}\right) = \left(\frac{-1}{g}\right). \tag{1.5}$$

We prove the following theorem.

THEOREM 1. *Let* $p \equiv 1$ (mod 8) *be a prime such that* $h(-p) \equiv 0$ (mod 8). *Set* $p = 2g^2 - h^2$, *where* g *and* h *are odd positive integers. As* $h(-p) \equiv 0$ (mod 8) *we have* $(-1/g) = (g/p) = +1$. *Then*

$$h(-p) \equiv 0 \ (\text{mod } 16) \Leftrightarrow \left(\frac{g}{p}\right)_4 = \left(\frac{2h}{g}\right).$$

Proof. We consider integral positive-definite binary quadratic forms $ax^2 + bxy + cy^2$ (written (a, b, c)) of discriminant $b^2 - 4ac = -4p$. Clearly b must be even. Moreover all such forms are primitive, that is, G.C.D $(a, b, c) = 1$. The class A of forms equivalent to the form (a, b, c) under an integral unimodular transformation of determinant $+1$ is written $A = [a, b, c]$. The product A_1A_2 of two such classes A_1 and A_2 is defined as follows: choose forms $(a_1, b, a_2c) \in A_1$ and $(a_2, b, a_1c) \in A_2$ and define A_1A_2 to be $[a_1a_2, b, c]$. These classes, with the multiplication specified above, form a finite abelian group $\mathscr{H}$, which is isomorphic to the class group $H(-p)$ of the imaginary quadratic field $Q(\sqrt{-p})$. Its order is the class number $h(-p)$.

The identity of $\mathscr{H}$ is the class $I = [1, 0, p]$ and the inverse class of $[a, b, c] \in \mathscr{H}$ is $[a, -b, c]$.

Setting $A = [2, 2, \frac{1}{2}(p+1)] \in \mathscr{H}$, $B = [g, 2h, 2g] \in \mathscr{H}$, it is easy to check that

$$B^2 = A \neq I, \qquad A^2 = I, \tag{1.6}$$

so that

$$\text{ord}(A) = 2, \qquad \text{ord}(B) = 4. \tag{1.7}$$

As $(g/p) = +1$, the form $(g, 2h, 2g)$ represents an integer s, namely $s = g$, satisfying

$$\left(\frac{-1}{s}\right) = \left(\frac{s}{p}\right) = +1, \qquad (s, 2p) = 1.$$

Thus B belongs to the principal genus of $\mathscr{H}$, and so, by Gauss' duplication theorem, is the square of some class $C = [l, m, n]$, that is,

$$C^2 = B. \tag{1.8}$$

https://doi.org/10.4153/CMB-1982-027-0 Published online by Cambridge University Press

Clearly we have

$$\text{(1.9)} \qquad \operatorname{ord}(C)=8.$$

Replacing (l, m, n) by an equivalent form, we can suppose that

$$\text{(1.10)} \qquad \text{G.C.D.}(l, 2gp)=1.$$

We will now show that

$$\text{(1.11)} \qquad h(-p)\equiv 0 (\operatorname{mod} 16) \Leftrightarrow \left(\frac{l}{p}\right)=+1.$$

If $(l/p)=+1$ then, as C represents l, C must belong to the principal genus, and so is the square of some class D. From (1.9) we have ord $(D)=16$, and so $h(-p)\equiv 0 \pmod{16}$.

Conversely if $h(-p)\equiv 0 \pmod{16}$, since the 2-Sylow subgroup of $\mathscr{H}$ is cyclic by a theorem of Gauss, $\mathscr{H}$ contains an element D of order 16. Thus D^2 is of order 8. But there are exactly four elements of order 8 in $\mathscr{H}$, namely C, C^3, C^5, C^7, thus we must have

$$D^2=C, C^3, C^5 \quad \text{or} \quad C^7.$$

In each case we see that C is a square and so C belongs in the principal genus. But C represents l so we must have $(l/p)=+1$. This completes the proof of (1.11). This technique of taking successive squareroots has been described by a number of authors [1], [5], [8], [10]. To complete the proof of the theorem we must show that

$$\text{(1.12)} \qquad \left(\frac{l}{p}\right)=\left(\frac{g}{p}\right)_4\left(\frac{2h}{g}\right).$$

Since l is represented primitively by the form (l, m, n) and $[l, m, n]^2=[g, 2h, 2g]$, l^2 is represented primitively by the form $(g, 2h, 2g)$. Thus there are integers x and y such that

$$\text{(1.13)} \qquad l^2=gx^2+2hxy+2gy^2, \qquad (x, y)=1.$$

Changing the signs of both x and y, if necessary, we can suppose that x is positive. Clearly x is odd. We set

$$\text{(1.14)} \qquad k=|hx+2gy|,$$

so that k is an odd positive integer. From (1.1), (1.13) and (1.14) we obtain

$$\text{(1.15)} \qquad 2gl^2=k^2+px^2,$$

so that k is not divisible by p. Using (1.2), (1.10), (1.13) and (1.15), it is easy to check that

(1.16)

$$\text{G.C.D.}(x, l)=\text{G.C.D.}(x, k)=\text{G.C.D.}(x, g)=\text{G.C.D.}(k, g)=\text{G.C.D.}(k, l)=1.$$

https://doi.org/10.4153/CMB-1982-027-0 Published online by Cambridge University Press

From (1.15) we have

$$\left(\frac{2gl^2}{p}\right)_4=\left(\frac{k^2}{p}\right)_4=\left(\frac{k}{p}\right)=\left(\frac{p}{k}\right)=\left(\frac{px^2}{k}\right)=\left(\frac{2gl^2}{k}\right),$$

so that

$$\left(\frac{l}{p}\right)=\left(\frac{2}{p}\right)_4\left(\frac{g}{p}\right)_4\left(\frac{2g}{k}\right). \tag{1.16}$$

Next from (1.1) and (1.2) we obtain

$$\left(\frac{2}{p}\right)_4=\left(\frac{2g^4}{p}\right)_4=\left(\frac{g^2h^2}{p}\right)_4=\left(\frac{gh}{p}\right)=\left(\frac{h}{p}\right)=\left(\frac{p}{h}\right)=\left(\frac{2g^2}{h}\right)=\left(\frac{2}{h}\right),$$

so that (1.16) becomes

$$\left(\frac{l}{p}\right)=\left(\frac{g}{p}\right)_4\left(\frac{2}{h}\right)\left(\frac{2}{k}\right)\left(\frac{g}{k}\right). \tag{1.17}$$

Further, from (1.1) and (1.15), we get

$$k^2-1=2gl^2-(2g^2-h^2)x^2-1\equiv 2g-2+h^2x^2-1 \pmod{16},$$

so that

$$\tfrac{1}{8}(k^2-1)\equiv\tfrac{1}{4}(g-1)+\tfrac{1}{8}(h^2x^2-1) \pmod 2,$$

giving

$$\left(\frac{2}{k}\right)=\left(\frac{2}{g}\right)\left(\frac{2}{hx}\right),$$

so that (1.17) gives

$$\left(\frac{l}{p}\right)=\left(\frac{g}{p}\right)_4\left(\frac{2}{g}\right)\left(\frac{2}{x}\right)\left(\frac{g}{k}\right). \tag{1.18}$$

Finally, we have (as $g\equiv 1 \pmod 4$)

$$\begin{aligned}\left(\frac{g}{k}\right)=\left(\frac{k}{g}\right)=\left(\frac{hx+2gy}{g}\right)=\left(\frac{hx}{g}\right)=\left(\frac{h}{g}\right)\left(\frac{g}{x}\right)\\ =\left(\frac{h}{g}\right)\left(\frac{4gl^2}{x}\right)=\left(\frac{h}{g}\right)\left(\frac{2k^2}{x}\right)=\left(\frac{h}{g}\right)\left(\frac{2}{x}\right),\end{aligned}$$

and using this in (1.18) we obtain

$$\left(\frac{l}{p}\right)=\left(\frac{g}{p}\right)_4\left(\frac{2h}{g}\right),$$

as required. This completes the proof of the theorem.

We remark that in a paper to appear elsewhere [12], the second author has

https://doi.org/10.4153/CMB-1982-027-0 Published online by Cambridge University Press

shown that if $p\equiv 1 \pmod 8$ is a prime such that $h(-p)\equiv 0 \pmod 8$, then $h(-p)\equiv T+p-1 \pmod{16}$, where $T+U\sqrt{p}$ is the fundamental unit of $Q(\sqrt{p})$.

We also note that Theorem 1 answers a question of Brown [4: p. 417].

2. $D=-2p$, $p\equiv 1 \pmod 8$. In the representation (0.1) clearly u is odd and v is even. Replacing (u, v) by the representation $(3u+4v, 2u+3v)$, if necessary, we can suppose that

$$u\equiv 1 \pmod 4. \tag{2.1}$$

By a theorem of Hasse [7: p. 234] [8: p. 5], we have

$$h(-2p)\equiv 0 \pmod 8 \Leftrightarrow u\equiv 1 \pmod 8 \Leftrightarrow \left(\frac{u}{p}\right)=+1. \tag{2.2}$$

Assuming that $h(-2p)\equiv 0 \pmod 8$, in view of (2.2), the symbol $(u/p)_4$ is well-defined and independent of the choice (u, v) satisfying (0.1) and the condition $u\equiv 1 \pmod 8$. Proceeding exactly as in the proof of Theorem 1, but with I, A, B replaced by $[1, 0, 2p]$, $[2, 0, p]$, $[u, 4v, 2u]$ respectively, we obtain

$$h(-2p)\equiv 0 \pmod{16} \Leftrightarrow \left(\frac{l}{p}\right)=+1,\ \left(\frac{l}{p}\right)=\left(\frac{u}{p}\right)_4,$$

which establishes the following theorem.

THEOREM 2. *Let $p\equiv 1 \pmod 8$ be a prime such that $h(-2p)\equiv 0 \pmod 8$. Set $p=u^2-2v^2$, where u and v are positive integers with u chosen to satisfy $u\equiv 1 \pmod 8$. Then*

$$h(-2p)\equiv 0 \pmod{16} \Leftrightarrow \left(\frac{u}{p}\right)_4=+1.$$

In a forthcoming paper [10], Kaplan and the second author have established a congruence modulo 16 involving $h(-2p)$ and $h(2p)$ (the narrow class number of the real quadratic field $Q(\sqrt{2p})$). Using this congruence together with Theorem 2 in the case when $p\equiv 1 \pmod 8$ is such that $h(2p)\equiv 0 \pmod 8$ (so that $p\equiv 1 \pmod{16}$) and one of the equations $x^2-2py^2=-1$ or $+2$ is solvable in integers x and y, we can obtain a necessary and sufficient condition for $h(2p)\equiv 0 \pmod{16}$.

COROLLARY. *Let $p\equiv 1 \pmod{16}$ be a prime such that $h(2p)\equiv 0 \pmod 8$ and such that one of the equations $x^2-2py^2=-1$, $+2$ is solvable in integers x and y. Set $p=u^2-2v^2$, where u and v are positive integers with u chosen so that $u\equiv 1 \pmod 8$. Then*

$$h(2p)\equiv 0 \pmod{16} \Leftrightarrow \left(\frac{u}{p}\right)_4=+1.$$

3. $D=-2p$, $p\equiv 7 \pmod 8$. In this case it is well-known that

$$h(-2p)\equiv\begin{cases}0 \pmod 8, & \text{if} \quad p\equiv 15 \pmod{16},\\ 4 \pmod 8, & \text{if} \quad p\equiv 7 \pmod{16},\end{cases} \tag{3.1}$$

see for example [2: Cor. 7.4], [7: p. 234].

We restrict our attention to primes $p\equiv 15 \pmod{16}$. From (0.1) we deduce that $u\equiv\pm 1 \pmod 8$. Replacing the representation (u, v) by $(3u+4v, 2u+3v)$, if necessary, we can suppose that $u\equiv 1 \pmod 8$. Replacing (u, v) by $(17u+24v, 12u+17v)$, if necessary, we can further suppose that $u\equiv 1 \pmod{16}$. Again proceeding exactly as in the proof of Theorem 1, we obtain

$$h(-2p)\equiv 0 \pmod{16} \Leftrightarrow \left(\frac{2}{l}\right)=+1, \left(\frac{2}{l}\right)=\left(\frac{v}{u}\right),$$

which establishes the following theorem.

THEOREM 3. *Let $p\equiv 15 \pmod{16}$ be a prime. Set $p=u^2-2v^2$, where u and v are positive integers with u chosen to satisfy $u\equiv 1 \pmod{16}$. Then*

$$h(-2p)\equiv 0 \pmod{16} \Leftrightarrow \left(\frac{v}{u}\right)=+1.$$

This result should be compared with the following result of the second author: if $p\equiv 15 \pmod{16}$ is prime then $h(-2p)\equiv U \pmod{16}$, where $T+U\sqrt{2p}$ is the fundamental unit of $Q(\sqrt{2p})$.

4. **Conclusion.** For $D<0$ there remains one further case when the 2-Sylow subgroup $H_2(D)$ of $H(D)$ is cyclic of order ≥ 4 (see for example [9]), namely,

$$D=-pq, \ p(\text{prime})\equiv 1 \pmod 4, \ q(\text{prime})\equiv 3 \pmod 4, \ \left(\frac{p}{q}\right)=+1. \tag{4.1}$$

In this case it is known (see for example [9: Théorème 8]) that

$$h(-pq)\equiv 0 \pmod 8 \Leftrightarrow \left(\frac{-q}{p}\right)_4=+1. \tag{4.2}$$

It would be interesting to obtain an explicit necessary and sufficient condition for $h(-pq)\equiv 0 \pmod{16}$ in this case too, but since (4.2) already involves the Dirichlet symbol $(-q/p)_4$ this may be difficult.

The authors would like to thank Pierre Kaplan of the University of Nancy, France for a helpful comment in connection with the proof of Theorem 1.
Kaplan [10] has obtained various criteria for the existence of cycles of order 16 in the class group of certain quadratic fields.

References

1. Helmut Bauer, *Zur Berechnung der* 2-*Klassenzahl der quadratische Zahlkörper mit genau zwei verschiedenen Diskriminantenprimteilern*, J. Reine Angew. Math. **248** (1971), 42–46.

2. Bruce C. Berndt, *Classical theorems on quadratic residues*, L'Enseignement Math. **22** (1976), 261–304.

3. 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.

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

5. Ezra Brown, *Class numbers of quadratic fields*, Symp. Mat. **15** (1975), 403–411.

6. Helmut Hasse, *Über die Klassenzahl des Körpers* $P(\sqrt{-p})$ *mit einer Primzahl* $p \equiv 1 \pmod{2^3}$, Aequationes Math. **3** (1969), 165–169.

7. Helmut Hasse, Über die Klassenzahl des Körpers $P(\sqrt{-2p})$ mit einer Primzahl $p \neq 2$, J. Number Theory 1 (1969), 231–234.

8. Helmut Hasse, Über die Teilbarkeit durch 2^3 der Klassenzahl imaginär-quadratischer Zahlkörper mit genau zwei verschiedenen Diskriminantenprimteilern, J. Reine Angew. Math. 241 (1970), 1–6.

9. Pierre Kaplan, Divisibilité par 8 du nombre des classes des corps quadratiques dont le 2-groupe des classes est cyclique, et réciprocité biquadratique, J. Math. Soc. Japan 25 (1973), 596–608.

10. Pierre Kaplan, Cycles d'ordre au moins 16 dans le 2-groupe des classes d'idéaux de certains corps quadratiques, Bull. Soc. Math. France Mém. No. 49–50 (1977), 113–124.

11. Pierre Kaplan and Kenneth S. Williams, On the class numbers of $Q(\sqrt{\pm 2p})$ modulo 16, for $p \equiv 1 \pmod 8$ a prime, Acta Arith. (to appear).

12. Kenneth S. Williams, On the class number of $Q(\sqrt{-p})$ modulo 16, for $p \equiv 1 \pmod 8$ a prime, Acta Arith. (to appear).

Arizona State University
Tempe, Arizona, U.S.A.
82581

Carleton University
Ottawa, Ontario, Canada
K1S 5B6

https://doi.org/10.4153/CMB-1982-027-0 Published online by Cambridge University Press