The quadratic fields with discriminant divisible by exactly two primes and with "narrow" class number divisible by 8

By Julius M. Basilla*)

Department of Mathematics, Sophia University
7-1 Kioicho, Chiyoda-ku, Tokyo 102-8554

(Communicated by Shigefumi Mori, M. J. A., Dec. 13, 2004)

Abstract: Let K be the quadratic field $\mathbf{Q}(\sqrt{m})$ with discirimant $d = pq$. Using Legendre's theorem on the solvability of the equation $ax^2+by^2 = z^2$, we give necessary and sufficient conditions for the class number of K in the narrow sense to be divisible by 8. The approach recovers known criteria but is simpler and can be extended to compute the sylow 2-subgroup of the ideal class group of quadratic fields.

Key words: Legendre's theorem; 2-part; Gauss genus theorem.

1. Preliminaries. Let m be a square free integer and K be the quadratic field $\mathbf{Q}(\sqrt{m})$ with discriminant d. Denote the narrow class number of K by h^+. For ideals $\mathfrak{a}$ and $\mathfrak{b}$, we write $\mathfrak{a} \cong \mathfrak{b}$ if $\mathfrak{a}$ and $\mathfrak{b}$ belong to the same ideal class in the narrow sense.

For integers a and b, we write $\left(\frac{a}{b}\right)_n = 1$ if $x^n \equiv a \pmod{b}$ has a solution and $\left(\frac{a}{b}\right)_n = -1$ if $x^n \equiv a \pmod{b}$ has no solution.

The sylow-2 subgroup of the ideal class group of K in the narrow sense is a nontrivial cyclic group in the following cases.

- Real Cases
  1. $m = pq$, $p \equiv q \pmod 4$,
  2. $m = p$, $p \equiv 3 \pmod 4$,
  3. $m = 2p$, $p \neq 2$.
- Imaginary Cases
  4. $m = -pq$, $p \equiv -q \equiv 1 \pmod 4$,
  5. $m = -p$, $p \equiv 1 \pmod 4$,
  6. $m = -2p$, $p \neq 2$,

where p and q denote some prime numbers.

It is known that:

Theorem 1. 1. *For $m = pq$, $p \equiv q \pmod 4$: 8 divides h^+ if and only if $\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = 1$ (cf. [10]).*

2. *For $m = p$, $p \equiv 3 \pmod 4$: The class number in wide sense h is odd and h^+ is divisible by 2 but not by 4.*
3. *For $m = 2p$, $p \neq 2$: 8 divides h^+ if and only if $p = a^2 + b^2 \equiv 1 \pmod 8$, $a \equiv \pm 1 \pmod 8$, $b \equiv 0 \pmod 8$, or equivalently, 8 divides h^+ if and only if $\left(\frac{2}{p}\right)_4 = 1$, $p \equiv 1 \pmod{16}$. (cf. [6]).*
4. *For $m = -pq$, $p \equiv -q \pmod 4$: $8|h^+$ if and only if $\left(\frac{-q}{p}\right)_4 = 1$.*
5. *For $m = -p$, $p \equiv 1 \pmod 4$: $8|h^+$ if and only if $p \equiv a^2 + b^2 \equiv 1 \pmod 8$ and $a + b \equiv \pm 1 \pmod 8$ (cf. [6]), or equivalently, $8|h^+$ if and only if $p \equiv 1 \pmod 8$ and $\left(\frac{-4}{p}\right)_8 = 1$ (cf. [1]).*
6. *And for $m = -2p$, $p \neq 2$: $8|h^+$ if and only if $p \equiv -1 \pmod{16}$, or if $\left(\frac{2}{p}\right)_4 = 1$, $p \equiv 1 \pmod 8$.*

Results for case 1 (cf. [10]) and case 4 (cf. [1]) were obtained using class field theory. By looking at the properties of quadratic forms, Kaplan (cf. [6]) was able to confirm cases 1, 4, 5, and 6, in addition to his criteria for case 3.

Using Ideal Theory and Legendre's theorem on the solvability of the diophantine equation $ax^2 + by^2 = z^2$ (cf. [5]), Nemenzo (cf. [7]) was able to arrive at Scholz result. In this paper, we shall give an elementary proof of Kaplan's assertion following Nemenzo's approach.

In passing, we also verify the Rédei-Reichard theorem (cf. [9]):

Theorem 2. Rédei-Reichard Theorem.

1. *For $m = pq$, $p \equiv q \pmod 4$, 4 divides h^+ if and only if $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = 1$.*
2. *For $m = p$, $p \equiv 3 \pmod 4$, 4 does not divide h^+.*
3. *For $m = 2p$, $p \neq 2$, 4 divides h^+ if and only if $p \equiv 1 \pmod 8$.*
4. *For $m = -pq$, $p \equiv -q \equiv 1 \pmod 4$, 4 divides*

2000 Mathematics Subject Classification. Primary 11R29; Secondary 11R11.

*) On study leave from the Department of Mathematics, University of the Philippines-Diliman.

h^+ if and only if $\left(\frac{p}{q}\right) = 1$.

5. *For $m = -p$, $p \equiv 1 \pmod 4$, 4 divides h^+ if and only if $p \equiv 1 \pmod 8$.*
6. *For $m = -2p$, $p \neq 2$, 4 divides h^+ if and only if $p \equiv \pm 1 \pmod 8$.*

The main idea is to find necessary and sufficient conditions for a given ideal to be equivalent to the square of some ideals in K. We determine how many of the four primitive integral ambiguous ideals in K are fourth powers. Observe that if $\mathfrak{i}$, $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{ab}$ are the four primitive integeral ambiguous ideals, $8|h^+$ if and only if $\mathfrak{a}$ and $\mathfrak{b}$ are fourth powers. It is interesting to note that this approach can be extended to compute the Sylow 2 subgroup of the ideal class group of quadratic fields (cf. [2–4]).

In this paper, we use the lowercase roman letters to denote rational integers and the German letters $\mathfrak{a}, \mathfrak{b}, \cdots$ to denote ideals. We will reserve German letter $\mathfrak{i}$ for the unit ideal.

2. The ideals which are equivalent to a square. If a and b are nonzero integers, we write aRb if a is a square modulo b. We denote the square free part of a by a_1.

Lemma 3. *Let $\mathfrak{a} = \left[a, \frac{b+\sqrt{d}}{2}\right]$, $N\mathfrak{a} = a > 0$, $a|(b^2 - d)/4$. The ideal $\mathfrak{a}$ is equivalent to the square of some ideal, written $\mathfrak{a} \cong \square$, if and only if for all odd prime p dividing m, we have*

$$\left(\frac{a_1}{p}\right) = 1 \quad \textit{if } p \nmid a_1, \quad \textit{and}$$

$$\left(\frac{-a_1 m/p^2}{p}\right) = 1 \quad \textit{if } p \mid a_1.$$

Proof. The ideal $\mathfrak{a} \cong \square$ if and only if

$$(2ax + by)^2 - d_1 y^2 = a_1 z^2 \tag{1}$$

has a nontrivial solution (cf. [8]). Since m is square free, we have $d_1 = m$. If $m > 0$, (1) has a nontrivial solution if and only if mRa_1, a_1Rm, $\frac{-a_1 m}{(a_1,m)^2}R(a_1, m)$ (cf. [5]). If $m < 0$, (1) has a nontrivial solution if and only if $a_1(2ax + by)^2 + (-a_1 m)y^2 = z^2$ has a nontrivial solution, which in turn has a nontrivial solution if and only if $a_1 R\frac{-a_1 m}{(a_1,m)^2}$, $\frac{-a_1 m}{(a_1,m)^2}Ra_1$, and mRa_1.

Since $a|(b^2 - d)/4$, it follows that mRa_1. Observe also that

$$a_1 Rm \Leftrightarrow a_1 R\frac{-a_1 m}{(a_1, m)^2}$$
$$\Leftrightarrow \text{for all odd prime } p \mid m,\ p \nmid a_1,$$
$$\left(\frac{a_1}{p}\right) = 1.$$
$$\frac{-a_1 m}{(a_1, m)^2}Ra_1 \Leftrightarrow \frac{-a_1 m}{(a_1, m)^2}R(a_1, m)$$
$$\Leftrightarrow \text{for all odd prime } p \mid (a_1, m),$$
$$\left(\frac{-a_1 m/p^2}{p}\right) = 1.$$

□

3. The case $m = p$, $p \equiv 3 \pmod 4$. The four primitive integral ambiguous of K are $\mathfrak{i}$, $\mathfrak{p} = [p, \sqrt{p}]$, $\mathfrak{q} = [2, 1 + \sqrt{p}]$ and $\mathfrak{pq}$. Since $\left(\frac{-1}{p}\right) = -1$, $\mathfrak{p} \ncong \square$. If follows that $2||h^+$ for all $m = p \equiv 3 \pmod 4$.

4. The case $m = 2p$, $p \neq 2$. The four primitive integral ambiguous of K are $\mathfrak{i}$, $\mathfrak{p} = [p, \sqrt{2p}]$, $\mathfrak{q} = [2, \sqrt{2p}]$ and $\mathfrak{pq} = (\sqrt{2p})$. From Lemma 3, we have $\mathfrak{q} \cong \square$ if and only if $\left(\frac{2}{p}\right) = 1$ or $p \equiv \pm 1 \pmod 8$; and $\mathfrak{p} \cong \square$ if and only if $\left(\frac{-2}{p}\right) = 1$ (i.e., $p \equiv 1$ or $3 \pmod 8$). Thus, $4|h^+$ if and only if $p \equiv 1 \pmod 8$.

Let $\mathfrak{a} = [a, b + \sqrt{2p}]$, $a|b^2 - 2p$, and $(a, 8p) = 1$. From Lemma 3, $\mathfrak{a} \cong \square$ if and only if $\left(\frac{a_1}{p}\right) = 1$.

Let $p \equiv 1 \pmod 8$ so that $\mathfrak{p}$ and $\mathfrak{q}$ are equivalent to squares. If $\mathfrak{a}^2 \cong \mathfrak{p}$, there exist relatively prime integers x and y such that $px^2 - 2y^2 = a^2$ (cf. [8]). Write $y = 2^k y'$, y' odd. From this equation, we get

$$\left(\frac{a_1}{p}\right) = \left(\frac{-2y^2}{p}\right)_4 = \left(\frac{2}{p}\right)_4 \left(\frac{y}{p}\right),$$
$$\left(\frac{y}{p}\right) = \left(\frac{y'}{p}\right) = \left(\frac{p}{y'}\right) = \left(\frac{a_1^2}{p}\right) = 1.$$

Therefore,

$$\left(\frac{a_1}{p}\right) = 1 \Leftrightarrow \left(\frac{2}{p}\right)_4 = 1 \Leftrightarrow p = c^2 + 64f^2,$$

for some integers c and f, by Dirichlet Theorem on the biquadratic character of 2 (cf. [5]).

If $\mathfrak{a}^2 \cong \mathfrak{q}$, there exist integers x and y such that $2x^2 - py^2 = a^2$. Since $a|b^2 - 2p$, we have $\left(\frac{a}{p}\right) = \left(\frac{2}{a}\right)$. Thus, $\left(\frac{a}{p}\right) = 1$ if and only if $a \equiv \pm 1 \pmod 8$. Hence $\mathfrak{a} \cong \square$ if and only if $a^2 \equiv 1 \pmod{16}$. By inspecting $2x^2 - py^2 = a^2$, we see that y is odd and therefore $2x^2 - 1 \equiv 1 \pmod 8$. Thus, x is also odd. If t is a prime dividing y, we have that $\left(\frac{2}{t}\right) = 1$. And therefore, we have $y^2 \equiv 1 \pmod{16}$. Since x is odd, we have $2x^2 \equiv 2 \pmod{16}$. It follows that $\mathfrak{a} \cong \square$ if and only if $p \equiv 1 \pmod{16}$.

Hence, $8|h^+$ if and only if $p = c^2 + f^2 \equiv 1 \pmod 8$ with $c \equiv \pm 1 \pmod 8$ and $f \equiv 0 \pmod 8$.

5. The case $m = -pq, p \equiv -q \equiv 1$ (mod 4). The four primitive integral ambiguous of K, $\mathfrak{i}$, $\mathfrak{p} = \left[p, \frac{p+\sqrt{-pq}}{2}\right]$, $\mathfrak{q} = \left[q, \frac{q+\sqrt{-pq}}{2}\right]$ and $\mathfrak{pq} = (\sqrt{-pq})$ satisfy $\mathfrak{i} \cong \mathfrak{pq} \not\cong \mathfrak{p} \cong \mathfrak{q}$. Thus it suffices to consider the ideal $\mathfrak{p}$ only. From Lemma 3, $\mathfrak{p} \cong \square$ if and only if $\left(\frac{p}{q}\right) = 1$. That is, $4|h^+$ if and only if $\left(\frac{p}{q}\right) = 1$.

Assume that $\left(\frac{p}{q}\right) = 1$ so that $\mathfrak{p} \cong \mathfrak{a}^2$, for some ideal $\mathfrak{a}$. Put $\mathfrak{a} = \left[a, \frac{b+\sqrt{-pq}}{2}\right]$, $a|(b^2+pq)/4$, $(a, 2pq) = 1$ and all prime divisors of a split. From Lemma 3, $\mathfrak{a} \cong \square$ if and only if $\left(\frac{a_1}{p}\right) = \left(\frac{a_1}{q}\right) = 1$. Observe that

$$\left(\frac{a_1}{p}\right)\left(\frac{a_1}{q}\right) = \left(\frac{p}{a_1}\right)\left(\frac{-1}{a_1}\right)\left(\frac{q}{a_1}\right) = \left(\frac{-pq}{a_1}\right) = 1,$$

since all prime divisors of a_1 split. Thus $\left(\frac{a_1}{p}\right) = \left(\frac{a_1}{q}\right)$ and therefore, it suffices for us to find necessary and sufficient conditions for $\left(\frac{a_1}{p}\right) = 1$.

Since $\mathfrak{a}^2 \cong \mathfrak{p}$, there exist relatively prime integers x and y such that $p(2x+y)^2 + qy^2 = 4a^2$ (cf. [8]). Note that since $p \equiv 1 \pmod 4$, we have $\left(\frac{2}{p}\right) = \left(\frac{-1}{p}\right)_4$. It follows that

$$\left(\frac{a_1}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{2a}{p}\right) = \left(\frac{-1}{p}\right)_4\left(\frac{qy^2}{p}\right)_4 = \left(\frac{-1}{p}\right)_4\left(\frac{q}{p}\right)_4\left(\frac{y}{p}\right) = \left(\frac{-q}{p}\right)_4\left(\frac{y}{p}\right).$$

If $y = 2^k y'$, where y' is odd, it follows that $\left(\frac{y'}{p}\right) = \left(\frac{p}{y'}\right) = 1$. Thus $\left(\frac{y}{p}\right) = \left(\frac{2}{p}\right)^k$. If $k = 0$, then $\left(\frac{y}{p}\right) = 1$. Suppose y is even so that x is odd. Expanding we get $px^2 + pxy + y^2\left(\frac{p+q}{4}\right) = a^2$. It follows that $pxy \equiv 0 \pmod 4$. If $p \equiv 1 \pmod 8$, then $\left(\frac{y}{p}\right) = 1$. If $p \equiv 5 \pmod 8$, we get $5 + 5xy \equiv 1 \pmod 8$, so $5xy \not\equiv 0 \pmod 8$. That is, $k = 0$ of $k = 2$ and therefore $\left(\frac{y}{p}\right) = 1$.

Therefore, $\left(\frac{a_1}{p}\right) = 1$ if and only if $\left(\frac{-q}{p}\right)_4 = 1$. Hence, $8|h^+$ if and only if $\left(\frac{-q}{p}\right)_4 = 1$.

6. The case $m = -p, p \equiv 1$ (mod 4). The four primitive integral ambiguous of K, $\mathfrak{i}$, $\mathfrak{p} = (\sqrt{-p})$, $\mathfrak{q} = [2, 1+\sqrt{-p}]$ and $\mathfrak{pq} = [2p, p+\sqrt{-p}]$ satisfy $\mathfrak{i} \cong \mathfrak{p} \not\cong \mathfrak{q} \cong \mathfrak{pq}$. This, it suffices to consider $\mathfrak{q}$ only. From Lemma 3, $\mathfrak{q} \cong \square$ if and only if $\left(\frac{2}{p}\right) = 1$ or $p \equiv 1 \pmod 8$, i.e. $4|h^+$ if and only if $p \equiv 1 \pmod 8$.

Assume $p \equiv 1 \pmod 8$ so that $\mathfrak{q} \cong \mathfrak{a}^2$ for some ideal $\mathfrak{a} = [a, b+\sqrt{-p}]$, $a|b^2+p$, $(a, 4p) = 1$. From Lemma 3, $\mathfrak{a} \cong \square$ if and only if $\left(\frac{a_1}{p}\right) = 1$. Since $\mathfrak{a}^2 \cong \mathfrak{q}$, there exist relatively prime integers x and y such that $(2x+y)^2 + py^2 = 2a^2$. Put $u = 2x+y$. We have

$$\left(\frac{a_1}{p}\right) = \left(\frac{2a}{p}\right) = \left(\frac{4a^2}{p}\right)_4 = \left(\frac{2u^2}{p}\right)_4 = \left(\frac{2}{p}\right)_4\left(\frac{u}{p}\right).$$

If y is even, we get $u^2 + py^2 \equiv 0 \pmod 4$ but $2a^2 \equiv 2 \pmod 4$. Thus y is odd, and so is u. Using the same argument in section §4, we can show that $y^2 \equiv 1 \pmod{16}$.

Since u is odd, we have $\left(\frac{u}{p}\right) = \left(\frac{p}{u}\right) = \left(\frac{2a^2}{u}\right) = \left(\frac{2}{u}\right)$. Therefore, $\left(\frac{u}{p}\right) \equiv 1$ if and only if $u \equiv \pm 1 \pmod 8$.

Write $p = c^2 + 16f^2$ where c is odd (cf. [1]). Since a is odd, $a^2 \equiv 1 \pmod 8$ and $2a^2 \equiv 2 \pmod{16}$. Considering the equation $u^2 + py^2 = 2a^2$ modulo 16, we get

$$u^2 + (c^2 + 16f^2)y^2 \equiv 2a^2 \pmod{16}$$
$$u^2 + c^2 \equiv 2 \pmod{16}$$
$$u^2 \equiv c^2 \equiv 1 \text{ or } 9 \pmod{16}.$$

Applying Dirichlet's theorem on the biquadratic character of 2, we get

$$\left(\frac{2}{p}\right)_4 = \left(\frac{u}{p}\right) = 1 \Leftrightarrow c^2 \equiv u^2 \equiv 1 \pmod{16}, \quad 2|f \quad \Leftrightarrow p = c^2 + 64f'^2, \quad p \equiv 1 \pmod{16} \quad \Rightarrow \left(\frac{-1}{p}\right)_8 = 1,$$

for some integer f', and on the other hand,

$$\left(\frac{2}{p}\right)_4 = \left(\frac{u}{p}\right) = -1 \Leftrightarrow c^2 \equiv u^2 \equiv 9 \pmod{16}, \quad f \text{ odd} \quad \Leftrightarrow p \equiv 9 \pmod{16}, \quad f \text{ odd} \quad \Rightarrow \left(\frac{-1}{p}\right)_8 = -1.$$

In any case, we have

$$\left(\frac{-4}{p}\right)_8 = \left(\frac{-1}{p}\right)_8\left(\frac{2}{p}\right)_4 = 1.$$

We note that the $c^2 \equiv u^2 \equiv 1 \pmod{16}$ if and only if $c \equiv \pm 1 \pmod 8$ and $c^2 \equiv u^2 \equiv 9 \pmod{16}$ if and only if $c \equiv \pm 3 \pmod 8$. Thus, we can equivalently claim that $8|h^+$ if and only if there exist integers c and p, c odd such that $p = c^2 + f^2 \equiv 1 \pmod 8$ and $c + f \equiv \pm 1 \pmod 8$.

7. The case $m = -2p$, $p \neq 2$. The four primitive integral ambiguous of K, $\mathfrak{i}$, $\mathfrak{p} = [p, \sqrt{-2p}]$, $\mathfrak{q} = [2, \sqrt{-2p}]$ and $\mathfrak{pq} = (\sqrt{-2p})$, satisfy $\mathfrak{i} \cong \mathfrak{pq} \ncong \mathfrak{p} \cong \mathfrak{q}$. Thus, it suffices to consider $\mathfrak{q}$ only. From Lemma 3, $\mathfrak{q} \cong \Box$ if and only if $\left(\frac{2}{p}\right) = 1$ or $p \equiv \pm 1 \pmod 8$, i.e. $4|h^+$ if and only if $p \equiv \pm 1 \pmod 8$.

Suppose $\mathfrak{a} = [a, b + \sqrt{-2p}]$ such that $(a, 8p) = 1$, $a|b^2 + 2p$ and $\mathfrak{a}^2 \cong \mathfrak{q}$. From Lemma 3, $\mathfrak{a} \cong \Box$ if and only if $\left(\frac{a_1}{p}\right) = 1$. Since $\mathfrak{a}^2 \cong \mathfrak{q}$, there exist integers x and y such that

$$2x^2 + py^2 = a^2. \tag{2}$$

If $p \equiv 1 \pmod 8$, using the same argument as in §4 and the Dirichlet's Theorem on the biquadratic character of 2, we get

$$\begin{aligned}\left(\frac{a_1}{p}\right) = 1 \Leftrightarrow \left(\frac{2}{p}\right)_4 = 1 \\ \Leftrightarrow p = c^2 + f^2 \equiv 1 \pmod 8,\end{aligned}$$

where c is odd and $8|f$.

If $p \equiv -1 \pmod 8$, we can follow the argument that proves $p \equiv 1 \pmod{16}$ in §4, to show that $p \equiv -1 \pmod{16}$.

These give us all the quadratic fiels with discriminant divisible by exactly two primes and with "narrow" class number divisible by 8.

References

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

[2] Basilla, J. M.: Doctoral Thesis. Sophia University. (Preprint).

[3] Basilla, J. M., and Wada, H.: On efficient computation of the 2-parts of the ideal class groups of quadratic fields. Proc. Japan Acad., **80A**, 191–193 (2004).

[4] Hasse, H.: An algorithm for determining the structure of the 2-Sylow-subgroups of the divisor class group of a quadratic number field. Symposia Mathematica (Convegno di Strutture in Corpi Algebrici, INDAM, Roma 1973), vol. XV, Academic Press, London, pp. 341–352 (1975).

[5] Ireland, K., and Rosen, M.: A Classical Introduction to Modern Number Theory. 2nd ed. Grad. Texts in Math., 84, Springer-Verlag, New York, pp. 64, 272–275 (1990).

[6] Kaplan, P.: 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**, 596–608 (1973).

[7] Nemenzo, F. R.: On a Theorem of Scholz on the class number of quadratic fields. Proc. Japan Acad., **80A**, 9–11 (2004).

[8] Nemenzo, F., and Wada, H.: An elementary proof of Gauss' genus theorem. Proc. Japan Acad., **68A**, 94–95 (1992).

[9] Rédei, L., and Reichardt, H.: Die Anzahl der durch 4 teilbaren invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers. J. Reine Angew. Math., **170**, 69–74 (1934).

[10] Scholz, A.: Über die Lösbarket der Gleichung $t^2 - Du^2 = -4$. Math. Z., **39**, 95–111 (1934).