An application of dihedral fields to representations of primes by binary quadratic forms

by

Pierre Kaplan* (Nancy), Kenneth S. Williams* (Ottawa) and Yoshihiko Yamamoto (Osaka)

1. Introduction. Let $H(m)$ denote the strict ideal class group of the quadratic field $\mathbb{Q}(\sqrt{m})$ of discriminant $m$. We have

$$H(m) \cong Z_{2^{\alpha_1}} \times Z_{2^{\alpha_2}} \times \ldots \times Z_{2^{\alpha_k}} \times G,$$

where the order $g$ of the group $G$ is odd and $Z_{2^n}$ denotes the cyclic group of order $2^n$.

Let $p$ be a prime number such that $\left(\frac{m}{p}\right) = 1$. Then $p$ is represented by two inverse classes $C_p$, $C_p^{-1}$ (or one ambiguous class) of binary quadratic forms of discriminant $m$. Gauss's theory of genera determines $C_p$ modulo squares in the composition class group of discriminant $m$.

In this paper we determine the class $C_p$ modulo fourth powers in the simplest case, namely when

$$H(m) \cong Z_{2^n} \times G, \quad n \geq 2,$$

and the class $C_p$ is a square, that is $p$ is a prime on which all the generic characters have the value $+1$. It is known (see for example [2]) that (1.2) occurs precisely for the following values of the discriminant $m$:

(I) $m = -4r$, $r$(prime) $\equiv 1$(mod 8);

(II) $m = -8r$, $r$(prime) $\equiv 1$(mod 8);

(III) $m = -8q$, $q$(prime) $\equiv 7$(mod 8);

(IV) $m = -qr$, $q$(prime) $\equiv 3$(mod 4), $r$(prime) $\equiv 1$(mod 4), $\left(\frac{q}{r}\right) = 1$;

(V) $m = 8r$, $r$(prime) $\equiv 1$(mod 8);

(VI) $m = qr$, $q$(prime) $\equiv r$(prime) $\equiv 1$(mod 4), $\left(\frac{q}{r}\right) = 1$.

* Research supported by Natural Sciences and Engineering Research Council of Canada Grant A-7233.
We define
$q = 1$ in case (I),
$q = 2$ in cases (II), (V),
$r = 2$ in case (III)
and
\[ k_q = \begin{cases} Q(\sqrt{-q}) & \text{in cases (I), (II), (III), (IV);} \\ Q(\sqrt{q}) & \text{in cases (V), (VI);} \end{cases} \]

\[ k_r = Q(\sqrt{r}); \quad k_m = Q(\sqrt{m}) \]

\[ K = Q(\sqrt{r}, \sqrt{m}) = \begin{cases} Q(\sqrt{r}, \sqrt{-q}) & \text{in cases (I) to (IV),} \\ Q(\sqrt{r}, \sqrt{q}) & \text{in cases (V), (VI).} \end{cases} \]

The strict class number of the quadratic field $Q(\sqrt{d})$ will be denoted by $h(d)$.

Throughout this paper the symbol $\left( \frac{x + y \sqrt{n}}{p} \right)$, where $n$ and $x^2 - ny^2$ are quadratic residues of the odd prime $p$, will be used both as a Legendre symbol, in which case $\sqrt{n}$ is interpreted as a rational integer modulo $p$, as well as (equivalently) the quadratic residue symbol $\left[ \frac{x + y \sqrt{n}}{p} \right]_2$ in the ring of integers of $Q(\sqrt{n})$, where $P$ is either of the two prime ideals dividing $p$.

We prove:

**Theorem 1.** Let $r$ be a prime $\equiv 1 (\text{mod } 8)$ and $p$ a prime satisfying
\[ \left( \frac{-1}{p} \right) = \left( \frac{p}{r} \right)^2 = 1, \]
so that $p$ is represented by the classes $C_p$ and $C_p^{-1}$ of discriminant $-4r$, and there exist integers $a$, $b$, $e$ and $f$ such that
\[ p = a^2 + b^2, \]
\[ p^{br} = e^2 - rf^2, \quad e > 0, \quad (e, f) = 1. \]

Then the class $C_p$ is a fourth power if, and only if, for any solutions of (1.3) and (1.4),
\[ \left( \frac{a + b \sqrt{-1}}{r} \right) = 1 \]
or, equivalently, $e + f = 1 (\text{mod } 4)$.

**Theorem 2.** Let $r$ be a prime $\equiv 1 (\text{mod } 8)$ and $p$ a prime satisfying
\[ \left( \frac{-2}{p} \right) = \left( \frac{p}{r} \right) = 1, \]
so that $p$ is represented by the classes $C_p$ and $C_p^{-1}$ of discriminant $-8r$, and there exist integers $a$, $b$, $e$ and $f$ such that
(1.5) \[ p = a^2 + 2b^2, \]
(1.6) \[ p^{h(q)} = e^2 - rf^2, \quad e > 0, \quad (e, f) = 1. \]

Then the class \( C_p \) is a fourth power if, and only if, for any solutions of (1.5) and (1.6), \[ \left( \frac{a+b\sqrt{-2}}{r} \right) = 1 \] or, equivalently, \[ \left( \frac{2}{p} \right)^{r-1/8} \left( \frac{-2}{e+f} \right) = 1. \]

**Theorem 3.** Let \( q \equiv 7 \pmod{8} \) be a prime. Let \( p \) be a prime satisfying \[ \left( \frac{p}{q} \right) = \left( \frac{2}{p} \right) = 1, \] so that \( p \) is represented by the classes \( C_p \) and \( C_p^{-1} \) of discriminant \(-8q\), and there exist integers \( a, b, e \) and \( f \) such that

(1.7) \[ p^{h(q)} = a^2 + qb^2, \quad (a, b) = 1, \quad a \text{ or } b \equiv 1 \pmod{4}, \]
(1.8) \[ p = e^2 - 2f^2, \quad e > 0. \]

Then the class \( C_p \) is a fourth power if, and only if, for any solutions of (1.7) and (1.8),

\[ \left( -1 \right)^{(q+1)/8} \left( \frac{2}{a+b} \right) = 1 \] or, equivalently, \[ \left( \frac{e+f\sqrt{2}}{q} \right) = 1. \]

We note that Theorem 3 of [1] is part of the special case \( q = 7 \) of our Theorem 3.

**Theorem 4.** Let \( q \equiv 3 \pmod{4} \) and \( r \equiv 1 \pmod{4} \) be primes such that \( \left( \frac{q}{r} \right) = 1. \) Let \( p \) be a prime satisfying \( \left( \frac{p}{q} \right) = \left( \frac{p}{r} \right) = 1, \) so that \( p \) is represented by the classes \( C_p \) and \( C_p^{-1} \) of discriminant \(-qr\) and there exist integers \( a, b, e \) and \( f \) such that

(1.9) \[ 4p^{h(q)} = a^2 + qb^2, \quad (a, b) = 1 \text{ or } 2, \]
(1.10) \[ 4p^{h(r)} = e^2 - rf^2, \quad (e, f) = 1 \text{ or } 2, \quad e > 0. \]

Then the class \( C_p \) is a fourth power if, and only if, for any solutions of (1.9) and (1.10),

\[ \left( \frac{a+b\sqrt{-q}}{r^2} \right) = 1 \] or, equivalently, \[ \left( \frac{e+f\sqrt{r}}{q} \right) = 1. \]

We note that Theorems 6 and 7 of [1] can be deduced as special cases of our Theorem 4 with \( q = 3, \) \( r = 13 \) and \( q = 11, \) \( r = 5, \) respectively.

**Theorem 5.** Let \( r \) be a prime \( \equiv 1 \pmod{8} \) and \( p \) be a prime satisfying \( \left( \frac{2}{p} \right) \)
\[ \left( \frac{p}{r} \right) = 1, \text{ so that } p \text{ is represented by the classes } C_p \text{ and } C_p^{-1} \text{ of discriminant } 8p, \text{ and that there exist integers } a, b, e \text{ and } f \text{ such that} \]
\begin{align*}
(1.11) \quad & p = a^2 - 2b^2, \quad (a, b) = 1, \quad a > 0; \\
(1.12) \quad & p^{(e) r} = e^2 - rf^2, \quad (e, f) = 1, \quad e+f \equiv 1 \pmod{4}. 
\end{align*}

Then \( C_p \) is a fourth power if, and only if, for any solutions of (1.11) and (1.12),
\[ \left( \frac{a+b\sqrt{q}}{r} \right) = 1 \text{ or, equivalently, } e+f \equiv 1 \pmod{8}. \]

**Theorem 6.** Let \( q \) and \( r \) be primes \( \equiv 1 \pmod{4} \) such that \( \left( \frac{q}{r} \right) = 1. \) Let \( p \) be a prime satisfying \( \left( \frac{p}{q} \right) = \left( \frac{p}{r} \right) = 1, \) so that \( p \) is represented by the classes \( C_p \) and \( C_p^{-1} \) of discriminant \( qr \) and that there exist integers \( a, b, e \) and \( f \) such that
\begin{align*}
(1.13) \quad & 4p^{(e) r} = a^2 - qb^2, \quad (a, b) = 1 \text{ or } 2; \\
(1.14) \quad & 4p^{(e) r} = e^2 - rf^2, \quad (e, f) = 1 \text{ or } 2. 
\end{align*}

Then \( C_p \) is a fourth power if, and only if, for any solutions of (1.13) and (1.14),
\[ \left( \frac{(a+b\sqrt{q})/2}{r} \right) = 1 \text{ or, equivalently, } \left( \frac{(e+f\sqrt{r})/2}{q} \right) = 1. \]

**2. Proof of the theorems.** The assumption (1.2) implies that the strict class group of \( k_m \) contains exactly one subgroup of index 4. Let \( L \) be the extension of \( k_m \) corresponding to this subgroup by class field theory. Then \( L \) is the cyclic extension of degree 4 of \( k_m \), unramified at any finite prime.

It is known ([3]) that \( L \) is a dihedral extension of \( Q \) whose quadratic subfields are \( k_m, k_q \) and \( k_r \) and whose quartic subfields are the field \( K \), two fields \( A \) and \( A' \) containing \( k_q \), but neither \( k_r \) nor \( k_m \), and two fields \( B \) and \( B' \) containing \( k_r \) but neither \( k_q \) nor \( k_m \).

\[ \begin{array}{c}
A' \\
\downarrow \\
K \\
\downarrow \\
A \\
\downarrow \\
Q \\
\downarrow \\
K_m \\
\downarrow \\
K_q \\
\downarrow \\
k_r \\
\downarrow \\
k_q \\
\downarrow \\
k_m \\
\downarrow \\
K \\
\downarrow \\
B' \\
\downarrow \\
B \\
\downarrow \\
Q \\
\downarrow \\
K_m \\
\downarrow \\
k_r \\
\downarrow \\
k_q \\
\downarrow \\
k_m
\end{array} \]

Let \( p \) be a prime on which all the generic characters of \( k_m \) take the value +1. Then \( p \) is completely decomposed in \( K \), the genus field of \( k_m \), and the classes \( C_p, C_p^{-1} \) are squares. The classes \( C_p, C_p^{-1} \) are fourth powers if, and
only if \( p \) is completely decomposed in \( L \), that is if \( p \) is completely decomposed in any of the four fields \( A, A', B \) or \( B' \).

Consider for instance the extension \( B/k_r \), of conductor \( f_B \). There exists a character \( \chi_B \) of order 2 on the group of ideals of \( k_r \) prime to \( f_B \) such that a prime ideal \( q \) of \( k_r \) is decomposed in \( B \) if, and only if, \( \chi_B(q) = 1 \). The value \( \chi_B(q) \) is equal to \( \chi_B((q^{2r})) \), as \( h(r) \) is odd, and the value of \( \chi_B \) on principal ideals prime to \( f_B \) has been calculated in Propositions 2.6 to 2.11 of [4]. Applying this to either of the ideals \( \bar{p}_1, \bar{p}_2 \) such that \((p) = \bar{p}_1 \bar{p}_2 \) in \( k_r \) we shall obtain the results for those theorems involving the integers \( e \) and \( f \). The results involving the integers \( a \) and \( b \) will be obtained by considering the extension \( A/k_q \). We give the details of the proof of Theorem 3, the other proofs are similar. In this case the decompositions of \( p, q \) and \( r = 2 \) in the fields \( k_q \) and \( k_r \) are the following:

\[
(2.1) \quad (p) = p_1 p_2, \quad (q) = (\sqrt{-q})^2, \quad (2) = r_1 r_2 \quad \text{in} \quad k_q,
\]

\[
(2.2) \quad (p) = \bar{p}_1 \bar{p}_2, \quad (q) = \bar{q}_1 \bar{q}_2, \quad 2 = (\sqrt{2})^2 \quad \text{in} \quad k_r.
\]

We first consider the extension \( A/k_q \). By Section 2 of [4] one of \( r_1, r_2 \) is ramified in \( A/k_q \) and the other in \( A'/k_q \); we choose the notation so that \( r_1 \) ramifies in \( A/k_q \). By Proposition 2.9 of [4] the conductor of \( A/k_q \) is \( r_1^2 \) and the value of the character \( \chi_A \) on principal ideals is given by:

\[
(2.3) \quad \chi_A((\lambda)) = \begin{cases} 
1, & \text{if } \lambda \equiv \pm 1 \pmod{r_1^2}, \\
-1, & \text{if } \lambda \equiv \pm 3 \pmod{r_1^2}.
\end{cases}
\]

Let \((a, b)\) be a solution of \( a^2 + b^2 q = p^{h(-q)} \). As the integers \( a + b \sqrt{-q} \) and \( a - b \sqrt{-q} \) are coprime we may set

\[
(2.4) \quad (a + b \sqrt{-q}) = p_1^{h(-q)}, \quad (a - b \sqrt{-q}) = p_2^{h(-q)}.
\]

Now from (2.3) we first see, as \( p \equiv \pm 1 \pmod{8} \), that:

\[
(2.5) \quad \chi_A(p_1) \chi_A(p_2) = \chi_A((p)) = 1,
\]

so that from (2.3) and the fact that \( h(-q) \) is odd:

\[
(2.6) \quad \chi_A(p_1) = \chi_A(p_2) = \begin{cases} 
1, & \text{if } a + b \sqrt{-q} \equiv \pm 1 \pmod{r_1^2}, \\
-1, & \text{if } a + b \sqrt{-q} \equiv \pm 3 \pmod{r_1^2}.
\end{cases}
\]

Let \( \beta = 1 \) or \( 3 \) be such that \( q \equiv -\beta^2 \pmod{16} \). As \( (\beta - \sqrt{-q})(\beta + \sqrt{-q}) \equiv 0 \pmod{r_1^2 r_2^2} \) and \( \beta - \sqrt{-q}, \beta + \sqrt{-q} \equiv 2 \) there exists \( \varepsilon = \pm 1 \) such that \( a + \varepsilon b \sqrt{-q} \equiv a + \varepsilon b \beta \pmod{r_1^2} \) and so

\[
\chi_A(p_1) = \begin{cases} 
1, & \text{if } a + \varepsilon b \beta \equiv \pm 1 \pmod{8}, \\
-1, & \text{if } a + \varepsilon b \beta \equiv \pm 3 \pmod{8},
\end{cases}
\]
that is

\[(2.7) \quad \chi_A(p_1) = \chi_A(p_2) = \left(\frac{2}{a+\sqrt{\beta h}}\right).\]

The integer \(a\) is odd or divisible by 4 according as \(p \equiv 1\) or \(-1\) (mod 8) so that when \(q \equiv -9\) (mod 16) we have

\[\left(\frac{2}{a+3\beta h}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{a+\beta h}\right)\]

which together with (2.7) proves

\[(2.8) \quad \chi_A(p_1) = \chi_A(p_2) = \left(\frac{-1}{p}\right)^{(q+1)/8}\left(\frac{2}{a+\beta h}\right).\]

We next consider the extension \(B/k_0\). By (2.1) of [4] we can suppose that \(q_1\) ramifies in \(B\) and \(q_2\) in \(B^\prime\). Then the character \(\chi_B\) is given by

\[(2.9) \quad \chi_B((\lambda)) = \left[\frac{\lambda}{q_1^{1/2}}\right]\times \text{sgn } \lambda.\]

Let \((e, f)\) be any solution of \(p = e^2 - 2f^2\) where \(e > 0\). Then we may set \(p_1 = (e+f\sqrt{2}), p_2 = (e-f\sqrt{2})\), and we deduce from (2.9) that

\[(2.10) \quad \chi_B(p_1) = \chi_B(p_2) = \left[\frac{e+f\sqrt{2}}{q_1}\right]_{q_1} = \left[\frac{e+f\sqrt{2}}{q}\right].\]

which together with (2.8) completes the proof of Theorem 3.

Remark. The class \(C_p\) of discriminant \(m\) is a fourth power or not according as \(p^{(m)/4}\) is represented by the principal class \(I\) or by the class \(J\) of order 2. Using the well-known representative of \(I\) and of \(J\), and also the forms of discriminant \(4m\) when \(m\) is odd, we obtain:

\[
\begin{align*}
\text{C}_p \text{ fourth power} & \quad \text{C}_p \text{ square, not fourth power} \\
\text{Theorem I} & \quad p^{n/4} = X^2 + rY^2 \quad 2p^{n/4} = X^2 + rY^2 \\
\text{Theorem II} & \quad p^{n/4} = X^2 + 2rY^2 \quad p^{n/4} = 2X^2 + rY^2 \\
\text{Theorem III} & \quad p^{n/4} = X^2 + 2qY^2 \quad p^{n/4} = 2X^2 + qY^2 \\
\text{Theorem IV} & \quad p^{n/4} = X^2 + XY + \frac{q+r+1}{4}Y^2 \quad p^{n/4} = qX^2 + qXY + \frac{q+r}{4}Y^2 \\
& \quad 4p^{n/4} = X^2 + qrY^2 \quad 4p^{n/4} = qX^2 + rY^2 \\
\text{Theorem V} & \quad p^{2n/4} = X^2 - 2rY^2 \quad g\beta^{2n/4} = X^2 - 2rY^2 \\
\text{Theorem VI} & \quad p^{n/4} = X^2 + X+ \frac{1-qr}{4}Y^2 \quad g\beta^{n/4} = X^2 + XY + \frac{1-qr}{4}Y^2 \\
& \quad 4p^{n/4} = X^2 - qrY^2 \quad 4g\beta^{n/4} = X^2 - qrY^2
\end{align*}
\]
In the cases (V), (VI) when \( m > 0 \) the integer \( g = -1 \), \( q \) or \( r \) is such that the solvable non pellian equation is \( X^2 - qrY^2 = g \).

**Acknowledgement.** We acknowledge the help of Mr. C. Frieser in calculating many numerical examples for us.

**References**


