Arch. Math., Vol. 36, 53–56 (1981) 0003-889X/81/3601-0004 $ 01.50+0.20/0

A representation problem involving binary quadratic forms

By

PHILIP A. LEONARD[1]) and KENNETH S. WILLIAMS[2])

We let $H(-D)$ denote the group under composition of classes of primitive positive-definite integral binary quadratic forms of discriminant $-D$, where D is a positive integer. The order of the group $H(-D)$ is denoted by $h(-D)$. Throughout this note we restrict our attention to discriminants $-D$ for which the largest odd divisor D' of D is squarefree and greater than 1, and for which all cycles in the 2-class group $H_2(-D)$ are of order $\leqq 4$.

If D' is expressible in the form $a^2 + b^2$, the Lengendre symbol $\left(\frac{a+b\sqrt{-1}}{p}\right)$ is well-defined for any prime $p \equiv 1 \pmod 4$ with $\left(\frac{D'}{p}\right) = +1$, where we are interpreting $\sqrt{-1}$ rationally as a root of the congruence $x^2 \equiv -1 \pmod p$. When $H_2(-D)$ is cyclic of order 4, that is, when $H(-D)$ has exactly two ambiguous classes, both in the principal genus, the symbol $\left(\frac{a+b\sqrt{-1}}{p}\right)$ can be used to distinguish between the representations of an odd power of p by the two ambiguous forms. This situation occurs precisely when

(i) $D = 4q$, q (prime) $\equiv 1 \pmod 8$, $h(-4q) \equiv 4 \pmod 8$ or

(ii) $D = 16q$, q (prime) $\equiv 5 \pmod 8$.

In case (i) the ambiguous forms are $I = [1, 0, q]$ and $A = [2, 2, \frac{1}{2}(q+1)]$ and in case (ii) they are $I = [1, 0, 4q]$ and $A = [4, 0, q]$. If p is a prime satisfying

$$\left(\frac{-1}{p}\right) = \left(\frac{p}{q}\right) = +1, \quad p^{h(-D)/4}$$

is represented primitively by I when $\left(\frac{a+b\sqrt{-1}}{p}\right) = +1$ and by A when $\left(\frac{a+b\sqrt{-1}}{p}\right) = -1$, where $q = a^2 + b^2$. This result can be deduced from Cases 1.1

[1]) Research partially supported by the Faculty Grant-in-Aid Program at Arizona State University.

[2]) Research partially supported by the Natural Sciences and Engineering Research Council of Canada under Grant A-7233.

and 1.3 of the Table in [5: pp. 684—685], since $(a + b\sqrt{-1})$. ε_q is a square, where ε_q denotes the fundamental unit of $Q(\sqrt{q})$ [1: p. 275]. (See also [4: p. 239] and Burde's law [2].)

In this note we treat the situation when D' is expressible as both $a^2 + b^2$ and $c^2 + 2d^2$. For primes $p \equiv 1 \pmod 8$ with $\left(\frac{D'}{p}\right) = +1$, the Legendre symbols $\left(\frac{a + b\sqrt{-1}}{p}\right)$ and $\left(\frac{c + d\sqrt{-2}}{p}\right)$ are both well-defined. We would like to use these symbols to distinguish representations of an odd power of p by ambiguous forms when there are exactly four ambiguous classes in $H(-D)$, all in the principal genus, that is, when $H_2(-D) = C(4) \times C(4)$. This situation occurs when $D = 128q$, where $q \equiv 1 \pmod 8$ is a prime such that $h(-8q) \equiv 4 \pmod 8$. In this case the ambiguous forms are $I = [1, 0, 32q]$, $A = [4, 4, 8q + 1]$, $B = [32, 0, q]$, $AB = [32, 32, q + 8]$. We obtain the following theorem.

Theorem. *Let* $q \equiv 1 \pmod 8$ *be a prime such that* $h(-8q) \equiv 4 \pmod 8$. *Set*

$$2q = a^2 + b^2, \qquad q = c^2 + 2d^2.$$

Let $p \equiv 1 \pmod 8$ *be a prime satisfying* $(p/q) = +1$. *Then* $p^{h(-8q)/4}$ *is represented primitively by*

$$\begin{aligned}
&I, && \text{if} \quad \left(\frac{a+b\sqrt{-1}}{p}\right) = \left(\frac{c+d\sqrt{-2}}{p}\right) = +1,\\
&A, && \text{if} \quad \left(\frac{a+b\sqrt{-1}}{p}\right) = -1, \quad \left(\frac{c+d\sqrt{-2}}{p}\right) = +1,\\
&B, && \text{if} \quad \left(\frac{a+b\sqrt{-1}}{p}\right) = (-1)^{(q-9)/8}, \quad \left(\frac{c+d\sqrt{-2}}{p}\right) = -1,\\
&AB, && \text{if} \quad \left(\frac{a+b\sqrt{-1}}{p}\right) = (-1)^{(q-1)/8}, \quad \left(\frac{c+d\sqrt{-2}}{p}\right) = -1.
\end{aligned}$$

We emphasize that to avoid a factor $(2/p)_4(p/2)_4$ the theorem is actually stated in terms of the representation $2q = a^2 + b^2$, rather than the representation $q = a^2 + b^2$. We illustrate the theorem by taking $q = 17$, so that $h(-8.17) = 4$, $a = 5$, $b = 3$, $c = 3$, $d = 2$. Let p be a prime satisfying

$$p \equiv 1, 9, 25, 33, 49, 81, 89, 121 \pmod{136}.$$

Then the theorem asserts that

$$p = x^2 + 544y^2 \Leftrightarrow \left(\frac{5+3\sqrt{-1}}{p}\right) = \left(\frac{3+2\sqrt{-2}}{p}\right) = +1,$$

$$p = 4x^2 + 4xy + 137y^2 \Leftrightarrow \left(\frac{5+3\sqrt{-1}}{p}\right) = -1, \quad \left(\frac{3+2\sqrt{-2}}{p}\right) = +1,$$

$$p = 32x^2 + 17y^2 \Leftrightarrow \left(\frac{5+3\sqrt{-1}}{p}\right) = \left(\frac{3+2\sqrt{-2}}{p}\right) = -1,$$

$$p = 32x^2 + 32xy + 25y^2 \Leftrightarrow \left(\frac{5+3\sqrt{-1}}{p}\right) = +1, \quad \left(\frac{3+2\sqrt{-2}}{p}\right) = -1.$$

For example, with $p = 281 \equiv 9 \pmod{136}$, we have

$$\left(\frac{5+3\sqrt{-1}}{p}\right) = \left(\frac{164}{281}\right) = -1, \quad \left(\frac{3+2\sqrt{-2}}{p}\right) = \left(\frac{61}{281}\right) = -1,$$

so that p is represented by the form $[32, 0, 17]$, and, indeed, $p = 32x^2 + 17y^2$ with $x = 2$, $y = 3$.

Proof of Thoerem. Set

$$p = a_1^2 + b_1^2, \quad a_1 \equiv 1 \pmod 2, \quad b_1 \equiv 0 \pmod 2,$$
$$q = a_2^2 + b_2^2, \quad a_2 \equiv 1 \pmod 2, \quad b_2 \equiv 0 \pmod 2,$$

so that we may take

$$a = a_2 + b_2, \quad b = a_2 - b_2.$$

Since

$$\left(\frac{b_1}{a_1}\right)^2 \equiv -1 \pmod p$$

we have, using [4: p. 323, Théorème 1, 2)],

$$\left(\frac{a+b\sqrt{-1}}{p}\right) = \left(\frac{aa_1 + bb_1}{p}\right) = \left(\frac{2q}{p}\right)_4 \left(\frac{p}{2q}\right)_4.$$

Now $p^{h(-8q)/4}$ is represented primitively by either $x^2 + 8qy^2$ or $8x^2 + qy^2$. In the first case, as $h(-8q)/4$ is odd, by a result of Kaplan [4: p. 361] we have

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

In the second case, by a similar calculation, we obtain

$$\left(\frac{2q}{p}\right)_4 \left(\frac{p}{2q}\right)_4 = (-1)^x \left(\frac{2}{q}\right)_4 \left(\frac{q}{2}\right)_4.$$

As $h(-8q) \equiv 4 \pmod 8$, we have $(2/q)_4 = -1$ [3: Théorème 3], so that

$$\left(\frac{2q}{p}\right)_4 \left(\frac{p}{2q}\right)_4 = \begin{cases} (-1)^x, & \text{if } q \equiv 9 \pmod{16}, \\ (-1)^{x+1}, & \text{if } q \equiv 1 \pmod{16}. \end{cases}$$

Hence, if $q \equiv 1 \pmod{16}$, we have:

$p^{h(-8q)/4}$ is represented primitively by

$$[1, 0, 32q] \quad \text{or} \quad [32, 32, q+8], \quad \text{if } \left(\frac{a+b\sqrt{-1}}{p}\right) = +1,$$

$$[4, 4, 8q+1] \text{ or } [32, 0, q], \qquad \text{if } \left(\frac{a+b\sqrt{-1}}{p}\right) = -1;$$

and, if $q \equiv 9 \pmod{16}$, we have:

$p^{h(-8q)/4}$ is represented primitively by

$$[1, 0, 32q] \quad \text{or} \quad [32, 0, q], \qquad \text{if } \left(\frac{a+b\sqrt{-1}}{p}\right) = +1,$$

$$[4, 4, 8q+1] \quad \text{or} \quad [32, 32, q+8], \text{ if } \left(\frac{a+b\sqrt{-1}}{p}\right) = -1.$$

Finally as $Q(\sqrt{-2q}, \sqrt{q}, \sqrt{c+d\sqrt{-2}})$ is (with $c+d\sqrt{-2}$ suitably normalized [6: p. 107]) the 4-class field for $Q(\sqrt{-2q})$, we have

$$\left(\frac{c+d\sqrt{-2}}{p}\right) = \begin{cases} +1, & \text{if } p^{h(-8q)/4} = x^2 + 8qy^2, \quad (x, y) = 1, \\ -1, & \text{if } p^{h(-8q)/4} = 8x^2 + qy^2, \quad (x, y) = 1. \end{cases}$$

This completes the proof of the theorem.

References

[1] J. A. BRANDLER, Residuacity properties of real quadratic units. J. Number Theory **5**, 271–286 (1973).

[2] K. BURDE, Ein rationales biquadratisches Reziprozitätsgesetz. J. Reine Angew. Math. **235**, 175–184 (1969).

[3] P. 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**, 596–608 (1973).

[4] P. KAPLAN, Sur le 2-groupe des classes d'idéaux des corps quadratiques. J. Reine Angew. Math. **283/284**, 313–363 (1976).

[5] PH. A. LEONARD and K. S. WILLIAMS, The quadratic and quartic character of certain quadratic units. II. Rocky Mountain J. Math. **9**, 683–692 (1979).

[6] PH. A. LEONARD and K. S. WILLIAMS, The quartic characters of certain quadratic units. J. Number Theory **12**, 106–109 (1980).

Eingegangen am 22. 4. 1980

Anschrift der Autoren:

Philip A. Leonard
Arizona State University
Tempe, Arizona 85281
USA

Kenneth S. Williams
Carleton University
Ottawa, Ontario K1S 5B6
Canada