JOURNAL OF NUMBER THEORY 5, 421–432 (1973)

Spinor Genera of Binary Quadratic Forms*

DENNIS R. ESTES

Department of Mathematics, University of Southern California, Los Angeles, California 90007

AND

GORDON PALL

Department of Mathematics, Louisiana State University, Baton Rouge, Louisiana 70803

PRESENTED AT THE QUADRATIC FORMS CONFERENCE, BATON ROUGE, LOUISIANA, MARCH 27–30, 1972, AND DEDICATED TO THE MEMORY OF LOUIS JOEL MORDELL

Spinor genera are defined for binary quadratic forms with integer coefficients in such a way that the theory fits in with the Gaussian theory of genera. It is shown that spinor generic characters exist which distinguish the various spinor genera in the principal genus, and how they can be determined. It is known that each ambiguous class contains exactly two forms of the type $[a, 0, c]$ or $[a, a, c]$, each with its associate $[c, 0, a]$, $[4c - a, 4c - a, c]$. Since the principal class contains such a form with $a = 1$, it is an interesting question whether one can predict the second form (not counting associates). This question includes that of Dirichlet about the representability of -1 by the principal class. Methods are given for evaluating the spinor-generic characters of ambiguous forms in the principal genus for variable discriminants d, and are carried through in the eleven cases where d is fundamental, there are two or four genera, and two spinor genera in the principal genus. The problem of determining the "second form" is thus completely solved except when there is more than one ambiguous class in the principal spinor genus.

1

A genus of primitive binary quadratic forms of nonzero discriminant d can be characterized by the property that if f and g are any of its forms, f can be transformed into g by means of a linear transformation with a rational matrix R of determinant ± 1 and with the least common denominator of its four elements prime to d. Since we can choose an equivalent form $[a, b, c] = ax^2 + bxy + cy^2$ with $(a, d) = 1$, and since replacing x

* This work was supported in part by N.S.F. grants GP-25735 and GP-2105X.

by $x + (b/a)y$ and y by $-y$ gives an automorph of $[a, b, c]$ of determinant -1, we can suppose that R has determinant $+1$.

Spinor genera of binary quadratic forms seem to have been little studied, yet numerous results in the literature now appear to be essentially spinor-generic phenomena. However, to make the theory dovetail with the Gaussian theory of genera it seems necessary to modify the usual definition of spinor genus, and to restrict the rational transformations to have determinant $+1$. We will say that two primitive binary quadratic forms are in the same *spinor genus* if they have the same nonzero discriminant d, and there exists a rational matrix R of determinant 1, norm 1, and denominator den R prime to d, such that $g = f^R$. Watson, in [1, p. 104], allows the determinant to be ± 1. With our definition, Watson's criterion [1, p. 105] becomes: *If f is a primitive binary quadratic form of nonzero discriminant d, and R is a rational matrix such that f^R is integral, $\det R = 1 = (d, \text{den } R)$, then f and f^R are in the same spinor genus if and only if there is a rational automorph S of determinant 1 and an integer q such that*

$$q^2(\text{den } R)(\text{den } S) \equiv 1 \pmod{d}. \tag{1}$$

Let f, g, h, i, j, k, l denote primitive binary quadratic forms of nonzero discriminant d. An equation such as $h = fg$ will mean that h is a product under Gaussian composition of f and g. We will prove

THEOREM 1. *If f and g are in the same spinor genus, and hence in the same genus, we can write $f = gh^2$. If $f = gh^2$, f and g are in the same spinor genus if and only if the genus of h contains an ambiguous class, hence if and only if $f = gk^4$ for some k.*

We will need

LEMMA 1. *The form f represents the square s^2 prime to d primitively if and only if $f = j^2$ where j represents s primitively.*

Proof. If $[s^2, b, c]$ is in the class of f, then $[s^2, b, c]$ is the square of $[s, b, sc]$, which is primitive since $(s, d) = 1$. Conversely, if $f = j^2$ choose a form $[a, b, c]$ in the class of j, $(a, d) = 1$. Then $(a, b) = 1$ and we can choose r so that $ar^2 + br + c \equiv 0 \pmod{a}$. Replacing x by $x + ry$ gives a form $[a, b', ac']$ in the class of j. Its square $[a^2, b', c']$ is in the class of f.

Suppose, in Theorem 1, that $f = kg$ where $k = h^2$. By the definition of Gaussian composition there is a bilinear substitution

$$\begin{aligned} y_1 &= t_{11}x_1z_1 + t_{12}x_2z_1 + t_{21}x_1z_2 + t_{22}x_2z_2, \\ y_2 &= s_{11}x_1z_1 + s_{12}x_2z_1 + s_{21}x_1z_2 + s_{22}x_2z_2, \end{aligned} \tag{2}$$

where the six minor determinants of order 2 are coprime, and if we regard (2) as a linear substitution with determinant $k(x_1, x_2)$ expressing y_1 and y_2 in terms of z_1 and z_2, then the substitution sends $f(y_1, y_2)$ into $k(x_1, x_2) \cdot g(z_1, z_2)$. Let u denote $t_{11}s_{12} - t_{12}s_{11}$. If $u = 0$ we can by a unimodular transformation on x_1 and x_2 suppose $t_{11} = s_{11} = 0$. Let t denote the first coefficient of k. Choose s primitively represented by h and prime to ud, or if $u = 0$ to td. By Lemma 1, k represents s^2 primitively. If $s^2 = k(r_1, r_2)$ where $(r_1, r_2) = 1$, then the matrix

$$T = \begin{bmatrix} (t_{11}r_1 + t_{12}r_2)/s & (t_{21}r_1 + t_{22}r_2)/s \\ (s_{11}r_1 + s_{12}r_2)/s & (s_{21}r_1 + s_{22}r_2)/s \end{bmatrix} \tag{3}$$

defines a transformation of determinant 1 and denominator s taking f into g. By the modified Watson criterion f and g will be in the same spinor genus if and only if f has a rational automorph S of determinant 1 and denominator v prime to d, with vs a square modulo d. It is known that the rational automorphs of determinant 1 of a primitive $f = [a, b, c]$ are given by

$$S = (1/t)\begin{bmatrix} p - (1/2)(b - e)q & -cq \\ aq & p + (1/2)(b + e)q \end{bmatrix} \tag{4}$$

where p and q are any coprime integers such that

$$p^2 + epq + (1/4)(e^2 - d)q^2 = t^2.$$

Here $e = 0$ or 1, $d \equiv e \pmod 4$. It is easy to verify that any factor of t which divides tS divides (a, b, c). Hence den $S = t$.

Suppose f and g are in the same spinor genus. Then there exist coprime p and q such that $p^2 + epq + (1/4)(e^2 - d)q^2 = t^2$, where $(t, d) = 1$ and ts is a square modulo d. Let U be a unimodular matrix with p q as first column. The transformation $y = Ux$ replaces the form $x_1^2 + ex_1x_2 + (1/4)(e^2 - d)x_2^2$ by $t^2y_1^2 + b_1y_1y_2 + c_1y_2^2$, which is l^2, where $l = [t, b_1, tc_1]$. Thus the class of l is ambiguous, and l and h are in the same genus since ts is a square modulo d.

Conversely, suppose that the genus of h contains an ambiguous class K. Choose in K a form l congruent to h modulo d. Let u, v be coprime integers such that $h(u, v) = s$, and set $t = l(u, v)$. Then the principal form represents t^2 primitively, and there exists a rational automorph S of f with determinant 1 and denominator t. Since $t \equiv s \pmod d$, f and g are in the same spinor genus.

Finally, if f and g are in the same spinor genus, $f = gh^2$ with h in the genus of an ambiguous form l, hl is in the principal genus, $hl = k^2$, $f = gh^2 = g(hl)^2 = gk^4$. And, if $f = gk^4$, k^2 is in the principal genus,

which obviously contains an ambiguous class, hence f and g are in the same spinor genus.

If $f_1 = f_2 h^4$ and $g_1 = g_2 k^4$, then $f_1 g_1 = (f_2 g_2)(hk)^4$. Hence,

COROLLARY 1. *The spinor genera form a group under the operation induced by class composition.*

Let C, G, S, S_1 denote the respective groups of primitive classes, primitive genera, spinor genera, and spinor genera in the principal genus.

COROLLARY 2. $C/C^4 \simeq S$, $C^2/C^4 \simeq S_1$, $C/C^2 \simeq S/S_1 \simeq G$.

Proof. The first isomorphism follows from Theorem 1 by the canonical map from C into S; the second follows from the first since every class in the principal genus is a square; the third from the first two since $G \simeq C/C^2$.

Since C^2/C^4 and C/C^2 are finite abelian groups in which every element is self-inverse, we may set $|S_1| = 2^u$, $|G| = 2^t$. Thus there are 2^{u+t} spinor genera and each genus contains 2^u spinor genera. Since the composition $G \to C/C^2 \to C^2/C^4 \to S_1$ has the kernel H we have

COROLLARY 3. *Let H be the subgroup of genera including at least one ambiguous class, $|H| = 2^n$. Then $S_1 \simeq G/H$ and $2^u = 2^{t-n}$.*

A nonambiguous class and its inverse represent exactly the same numbers, yet can be in different spinor genera. For example, if the 2-Sylow subgroup of C is cyclic of order 4, with K as generator, there are two spinor genera in the principal genus, including, respectively, I and K^2, and two in the second genus, including, respectively, K and K^3. On the other hand, $L^2 = L^{-2}L^4$ for any L, and hence,

COROLLARY 4. *In the principal genus any class and its inverse are in the same spinor genus.*

It may therefore be useful to study conditions for primes to be represented by spinor genera in the principal genus, since a prime is representable by at most one class and its inverse. Such conditions appear for a special case in the second of three articles by Dirichlet dealing—as we now recognize—with spinor-generic phenomena [2].

2

Generic characters and spinor-generic characters. The characterization of a genus by "rational equivalence without essential denominator" is very fine, but for some purposes, as for example the question of what

genera exist, it is necessary to use computable invariants. Gauss defined a primitive genus as consisting of all primitive forms with a given discriminant and index, and having common values for certain invariants called *generic characters*. To describe these conveniently we will use colons instead of lines in writing Legendre–Jacobi symbols, and will define [9]

$$\begin{aligned} (m : -1) = (-1 : m) &= 1 \quad \text{if} \quad m \equiv 1 \bmod 4, \\ &= -1 \quad \text{if} \quad m \equiv 3 \bmod 4; \end{aligned} \tag{6}$$

$$\begin{aligned} (m : 2) = (2 : m) &= 1 \quad \text{if} \quad m \equiv 1 \text{ or } -1 \bmod 8, \\ &= -1 \quad \text{if} \quad m \equiv 3 \text{ or } -3 \bmod 8; \end{aligned} \tag{7}$$

$$\begin{aligned} (m : -2) = (-2 : m) &= 1 \quad \text{if} \quad m \equiv 1 \text{ or } 3 \bmod 8, \\ &= -1 \quad \text{if} \quad m \equiv 5 \text{ or } 7 \bmod 8. \end{aligned} \tag{8}$$

Then, first, there is a generic character $(f : p)$ for each odd prime p dividing the discriminant d; that is, $(m : p)$ has a fixed value (1 or -1) for all integers m prime to p represented by the form f; and one writes $(f : p) = 1$ or -1 accordingly. Likewise, there is a generic character $(f : -1)$ when $d \equiv 0$ or $-4 \bmod 16$, $(f : 2)$ when $d \equiv 0$ or $8 \bmod 32$, $(f : -2)$ when $d \equiv 0$ or $-8 \bmod 32$; and each is evaluated by replacing the form symbol f by an odd integer m represented by f. It might be said here that we are using -1, 2, and -2 as conventional odd primes. It will be convenient to *omit* $(f : -2)$ from our *enumeration* of the generic characters when $d \equiv 0 \bmod 32$, since then $(f : -2) = (f : -1)(f : 2)$ (and all three *exist*). Let $t + 1$ be the number of generic characters so enumerated for a given discriminant d, and let the "primes" be $p_1, \ldots, p_{t+1}$. Notice that a product of generic characters is also an invariant of a genus. We will use the term *generic character* to include any of the 2^{t+1} products of the $t + 1$ generic characters $(f : p_i)$ enumerated earlier. Of course the even powers are trivially $+1$. We may write such symbols as $(f : -15)$ for $(f : -1)(f : 3)(f : 5)$. The factors must of course be generic invariants.

There are in fact, as Gauss proved, only 2^t primitive genera for a given discriminant (leaving aside the case where d is a square, and omitting negative-definite forms when $d < 0$). The reason for this is that the possible values of the enumerated generic characters $(f : p_i)$ are subject to the relation

$$(f : p_1)^{e_1} \cdots (f : p_{t+1})^{e_{t+1}} = 1, \tag{9}$$

where each exponent e_i is 0 or 1 as follows: set $d = -2^e D$, D odd; e_i is the residue mod 2 of the exponent to which p_i divides d if p_i is odd or p_i

is 2; of $(D+1)/2$ if $p_i = -1$; and $e_i = 1$ if $p_i = -2$ and $d \equiv -8 \bmod 32$. If d is square, all the exponents in (9) are even; and if f is negative-definite, the product there equals -1. When $d\ (\neq 1)$ is fundamental, every e_i is 1, and then, negative forms excluded, each generic character equals its complement (for example if $t = 3$, $(f : p_2) = (f : p_1)(f : p_3)(f : p_4)$). If d is nonsquare, at least one exponent in (9) is odd.

Notice that each of the 2^{t+1} generic characters is a character on the group C in the usual sense in group theory, with the value $+1$ on C^2 and constant on each genus. If d is nonsquare, and negative forms are omitted when $d < 0$, the number of distinct characters is 2^t.

The *spinor-generic characters* of a form f in the principal genus are defined to be the generic characters having common values for all the forms h such that $f = h^2$ (h nonnegative if $d < 0$). We will prove

THEOREM 2. *Let d be nonsquare. There exist spinor-generic characters on C^2 having the value 1 or -1 on each class in C^2, the value 1 on the principal spinor genus C^4, constant within each spinor genus of the principal genus, and together serving to distinguish between any two spinor genera in the principal genus. The number of spinor-generic characters is 2^{t-n+1} with t as above and n in Corollary* 3.

Proof. We have $h^2 = k^2$ if and only if $h = kg$ for some ambiguous g. Hence all we have to do is to show how to construct $t - n + 1$ independent generators for the group of generic characters having the value 1 on each genus containing an ambiguous class, and to show that these generators serve to distinguish the spinor genera in the principal genus. Set $h_0 = I$, and for $n > 0$, let $h_1, \ldots, h_n$ be generators, necessarily independent, of the group of genera containing an ambiguous class. We will show by induction that there are independent generic characters $\chi_i, \ldots, \chi_{t+1}$, $i = 1, \ldots, n+1$, which have the value 1 on and only on the group generated by $h_0, \ldots, h_{i-1}$, and which generate the generic characters that have the value 1 on the ambiguous classes. The theorem then follows by taking $i = n + 1$. We begin the induction with $i = 1$ by taking $\chi_1, \ldots, \chi_{t+1}$ to be a set of generators for the generic characters. Now suppose that appropriate characters $\chi_i, \ldots, \chi_{t+1}$ have been selected for a value i, $1 \leqslant i \leqslant n$, and renumber the subscripts so that $\chi_i, \ldots, \chi_m$ are those with value -1 on h_i. (This must occur, for if $\chi_i, \ldots, \chi_{t+1}$ have the value 1 on h_i, then by the hypothesis, h_i is in the group generated by $h_0, \ldots, h_{i-1}$, and $h_1, \ldots, h_i$ would not be independent.) There are two cases to consider, $m = i$ and $m > i$.

If $m = i$, drop χ_i and notice that if χ has the value 1 on the ambiguous classes then $\chi = \chi_i^{e_i}, \ldots, \chi_{t+1}^{t+1}$ and $1 = \chi(h_i) = (-1)^{e_i}$. Thus e_i is even and χ is therefore in the group generated by $\chi_{i+1}, \ldots, \chi_{t+1}$. Also, if $\chi_{i+1}(g) = \cdots = \chi_{t+1}(g) = 1$, then g or gh_i is in the group generated by $h_0, \ldots, h_{i-1}$ according as $\chi_i(g) = 1$ or -1. In either case, g is in the group generated by $h_1, \ldots, h_i$.

If $m > i$, set $\varphi_{i+1} = \chi_i\chi_{i+1}, \ldots, \varphi_m = \chi_i\chi_m$, $\varphi_{m+1} = \chi_{m+1}, \ldots, \varphi_{t+1} = \chi_{t+1}$ (all with the value 1 at h_i). Again, if $\chi = \chi_i^{e_i} \cdots \chi_{t+1}^{e_{t+1}}$ is 1 on all ambiguous classes, then

$$\chi = \chi_i^{e_i+e_{i+1}+\cdots+e_m}(\chi_i\chi_{i+1})^{e_{i+1}} \cdots (\chi_i\chi_m)^{e_m} \chi_{m+1}^{e_{m+1}} \cdots \chi_{t+1}^{e_{t+1}},$$

hence $e_i + \cdots + e_m$ is even and χ is expressible in terms of $\varphi_{i+1}, \ldots, \varphi_{t+1}$. Now let $\chi_{i+1}(g) = \cdots = \chi_{t+1}(g) = 1$. If $\chi_i(g) = 1$, $\chi_j(g) = \varphi_j(g)$, $i \leqslant j \leqslant t+1$, hence g is in the group generated by $h_0, \ldots, h_{i-1}$. If $\chi_i(g) = -1$, $\chi_i(gh_i) = 1$, $\chi_j(gh_i) = \chi_j(gh_i)\,\chi_i(gh_i) = \varphi_j(gh_i) = 1$ for $i < j \leqslant m$, and $\chi_j(gh_i) = \varphi_j(gh_i) = 1$ for $m < j \leqslant t+1$. Thus gh_i is in the group generated by $h_0, \ldots, h_{i-1}$. Finally, it is obvious that $\varphi_{i+1}, \ldots, \varphi_{t+1}$ are independent.

As an example consider $d = -4.7.23.17$. There are four genera containing (in this case actually consisting of) ambiguous classes, and four with nonambiguous classes, as follows, the generic characters being taken in the order 7, 23, 17, -1: $I = [1, 0, 2737]$, $J = [2, 2, 1369]$, $+\ +\ +\ +$; $A = [7, 0, 391]$, $JA = [14, 14, 199]$, $-\ -\ -\ -$; $B = [23, 0, 119]$, $JB = [46, 46, 71]$, $+\ +\ -\ -$; $AB = [17, 0, 161]$, $JAB = [34, 34, 89]$, $-\ -\ +\ +$; $[37, \pm 2, 74]$, $+\ -\ -\ +$; $[41, \pm 32, 73]$, $-\ +\ -\ +$; $[43, \pm 24, 67]$, $+\ -\ +\ -$; $[47, \pm 12, 59]$, $-\ +\ +\ -$. Take $h_1 = A$, $h_2 = B$. With A we get 7, 23, 17, -1; -7, -23, -17. Rearranging for B we get -17, -7, -23; -17, 161. Thus $\chi = (f^{1/2} : -17) = (f^{1/2} : 161)$ are the spinor-generic characters. Since J represents 37^2 primitively, $\chi(J) = (37 : -1)(37 : 17) = -1$, and I and J are in different spinor genera.

It will be useful in what follows to notice that *a square primitively represented is prime to d when d is fundamental, and otherwise can have no prime factors p in common with d except those for which d/p^2 is a discriminant.* (*Proof.* Study $[m^2, b, c]$, where $d = b^2 - 4m^2c$.)

3. SOME APPLICATIONS

The Gaussian reduction theory (see [3, p. 526]) easily implies that each primitive ambiguous class of positive nonsquare discriminant d contains exactly two pairs of forms of the type

$$[a, 0, c] \quad \text{or} \quad [a, a, c], \tag{10}$$

the associates being $[c, 0, a]$, $[4c - a, 4c - a, c]$, respectively. The principal form $[1, 0, c]$ or $[1, 1, c]$ is of this type. Hence the principal class must contain, associates apart, exactly one other form of type (10). This raises an interesting question: *what is the second form*? This may be called the *extended Dirichlet problem*, since it includes as a special case his celebrated problem of finding criteria for the principal class to represent -1. Much of the literature on his problem contains partial results unnoticed on the extended problem.

It should be pointed out that there are algorithms for computing the second form for any given discriminant d. The Gaussian reduction theory serves this purpose, although the computations may be tedious. There is a recent noteworthy technique due to Daniel Shanks [8].

Our idea is simply to try to construct spinor-generic characters for generators of the set of forms (10) in the principal genus. When there is only one other form (disregarding associates) all of whose spinor-generic characters have the value 1, that form must be in the principal class and the problem is solved. When there is more than one such form, our method fails to provide a criterion.

We will present the details here in all the eleven cases where d is fundamental, there are two or four genera, and two spinor genera in the principal genus. When d is odd we will use instead the discriminant $4d$ which gives equivalent results (see the second line on p. 529 of [3]) since it has the same generic characters as d. In each of the eleven cases there is essentially only one spinor character χ, and we have to consider three forms f, g, and fg of type (10) besides the principal form I. In each case, *if* $\chi(f)$ *or* $\chi(g)$ *equals* -1,

$$I \sim f \text{ if } \chi(f) = 1, \qquad I \sim g \text{ if } \chi(g) = 1, I \sim fg \text{ if } \chi(fg) = 1. \quad (11)$$

If $\chi(f) = \chi(g) = 1$, *our method fails to predict how the forms pair off.*

We will use the symbol $(q : p)_4$, where p is a prime congruent to 1 mod 4, $(q : p) = 1$, and if $q \equiv u^2 \bmod p$, $(q : p)_4 = (u : p)$. The symbol extends multiplicatively in the familiar way to $(a : b)_4$ where b is a product of primes $4n + 1$ and a is a quadratic residue of those primes. We will make much use of the two following lemmas.

LEMMA 5. *Let a and b be positive and coprime, and let a be a product of primes $4n + 1$. If $ax^2 - by^2 = z^2$ with x, y, z positive and $(x, y) = (z, 2ab) = 1$, then $(z : a) = (b : a)_4$ if either $a \equiv 1 \bmod 8$ or $b \equiv 1 \bmod 4$.*

Proof. Raising the congruence $-by^2 \equiv z^2 \bmod p$ to the power $(p - 1)/4$ for any prime p dividing a gives $(-1 : p)_4(b : p)_4(y : p) = (z : p)$; and taking the product for all such p gives $(-1 : a)_4(b : a)_4(y : a) = (z : a)$.

Set $y = 2^s y'$, y' odd. Then $(y : a) = (2 : a)^s(a : y') = (2 : a)^s$ since $ax^2 \equiv z^2 \bmod y'$. If $a \equiv 1 \bmod 8$, $(2 : a) = (-1 : a)_4 = 1$; if $a \equiv 5 \bmod 8$ and $b \equiv 1 \bmod 4$, then $s \equiv 1$ and $(-1 : a)_4 = (2 : a) = -1$.

LEMMA 6. *Write $(-1 : m)_8 = (-1)^{(m-1)/8}$ if $m \equiv 1 \bmod 8$. Let a and b be positive and coprime, $a \equiv 1 \bmod 8$, b divisible by no primes not of the form $4n + 1$. If $2bx^2 - ay^2 = z^2$ with x, y, z positive, $(x, y) = (z, 2ab) = 1$, then $(z : a) = (a : b)_4(-1 : a)_8$.*

Proof. We have $2bx^2 \equiv ay^2 \bmod z$, $(z : a) = (a : z) = (2 : z)(b : z) = (2 : z)(z : b)$, where as in Lemma 5, $(z : b) = (-1 : b)_4(a : b)_4(y : b)$ and $(y : b) = (b : y) = (2 : y)$. Also,

$$y^2 + z^2 \equiv 2bx^2 - (a - 1)y^2 \equiv 2b - (a - 1) \bmod 16,$$

hence $(2 : y)(2 : z) = (-1)^{(2b-(a-1)-2)/8} = (-1 : b)_4(-1 : a)_8$. The lemma follows.

Let p, q, r denote distinct odd primes. The eleven cases we will solve are as follows: (i) $d = 8p$, $p \equiv 1 \bmod 8$; (ii) $d = 4pq$, $p \equiv q \equiv 1 \bmod 4$, $(p : q) = 1$; (iii) $d = 8pq$, $p \equiv q \equiv 1 \bmod 8$, $(p : q) = -1$; (iv) $d = 4pqr$, $p \equiv q \equiv r \equiv 1 \bmod 4$, $(p : q) = (p : r) = -(q : r) = 1$; (v) $d = 8pq$, $p \equiv 1$, $q \equiv 5 \bmod 8$, $(p : q) = 1$; (vi) $d = 4pq$, $p \equiv 1$, $q \equiv 7 \bmod 8$, $(p : q) = 1$; (vii) $d = 8pq$, $p \equiv 1$, $q \equiv 7 \bmod 8$, $(p : q) = 1$; (viii) $d = 4pq$, $p \equiv 1$, $q \equiv 3 \bmod 8$, $(p : q) = 1$; (ix) $d = 8pq$, $p \equiv 1$, $q \equiv 3 \bmod 8$, $(p : q) = 1$; (x) $d = 8pq$, $p \equiv q \equiv 7 \bmod 8$, $(q : p) = 1$; (xi) $d = 4pqr$, $p \equiv 1$, $q \equiv r \equiv 3 \bmod 4$, $(p : q) = (p : r) = (q : r) = 1$.

The four forms (10) in the principal genus, and the spinor character, are:

	I	f	g	fg	χ
(i)	$[1, 0, -2p]$	$[p, 0, -2]$	$[-p, 0, 2]$	$[-1, 0, 2p]$	$(k^{1/2} : p) = (k^{1/2} : 2)$
(ii)	$[1, 0, -pq]$	$[p, 0, -q]$	$[-p, 0, q]$	$[-1, 0, pq]$	$(k^{1/2} : p) = (k^{1/2} : q)$
(iii)	$[1, 0, -2pq]$	$[-2, 0, pq]$	$[2, 0, -pq]$	$[-1, 0, 2pq]$	$(k^{1/2} : pq) = (k^{1/2} : 2)$
(iv)	$[1, 0, -pqr]$	$[p, 0, -qr]$	$[-p, 0, qr]$	$[-1, 0, pqr]$	$(k^{1/2} : qr) = (k^{1/2} : p)$
(v)	$[1, 0, -2pq]$	$[p, 0, -2q]$	$[-p, 0, 2q]$	$[-1, 0, 2pq]$	$(k^{1/2} : p) = (k^{1/2} : 2q)$
(vi)	$[1, 0, -pq]$	$[p, 0, -q]$	$[2, 2, \frac{1}{2}(1 - pq)]$	$[2p, 2p, \frac{1}{2}(p - q)]$	$(k^{1/2} : p) = (k^{1/2} : -q)$
(vii)	$[1, 0, -2pq]$	$[p, 0, -2q]$	$[2, 0, -pq]$	$[2p, 0, -q]$	$(k^{1/2} : p) = (k^{1/2} : -2q)$
(viii)	$[1, 0, -pq]$	$[p, 0, -q]$	$[-2, -2, \frac{1}{2}(pq - 1)]$	$[2q, 2q, \frac{1}{2}(q - p)]$	$(k^{1/2} : p) = (k^{1/2} : -q)$
(ix)	$[1, 0, -2pq]$	$[p, 0, -2q]$	$[-2, 0, pq]$	$[-2p, 0, q]$	$(k^{1/2} : p) = (k^{1/2} : -2q)$
(x)	$[1, 0, -2pq]$	$[2, 0, -pq]$	$[-2p, 0, q]$	$[2q, 0, -p]$	$(k^{1/2} : pq) = (k^{1/2} : 2)$
(xi)	$[1, 0, -pqr]$	$[p, 0, -rq]$	$[q, 0, -rp]$	$[pq, 0, -r]$	$(k^{1/2} : qr) = (k^{1/2} : p)$

(i) By Lemmas 5 and 6, $\chi(f) = (2 : p)_4$, $\chi(g) = (-1 : p)_8$.

(ii) By Lemma 6, $\chi(f) = (q : p)_4$ and $\chi(g) = (p : q)_4$, $\chi(fg) = (p : q)_4(q : p)_4$.

There follows forthwith a theorem due to Burde [4].

COROLLARY 7. *Let p, q be distinct primes of the form $4n + 1$, $(p : q) = 1$. Set $pq = a^2 + b^2$, a odd. Then $(p : q)_4(q : p)_4 = (a : p)$.*

Proof. $-b^2 + pq \cdot 1^2 = a^2$, hence $\chi(fg) = (a : p)$.

(iii) By Lemma 5, $\chi(f) = (2 : pq)_4$; by Lemma 6, $\chi(g) = (-1 : pq)_8$.

(iv) By Lemma 5, $\chi(f) = (qr : p)_4$, $\chi(g) = (p : qr)_4$.

(v) By Lemma 5, $\chi(f) = (2q : p)_4$; by Lemma 6, $\chi(g) = (p : q)_4(-1 : p)_8$.

In (vi) and (viii), $\chi(f) = (q : p)_4$; in (vii) and (ix), $\chi(f) = (2q : p)_4$. In (vi) and (vii) we will set $p = a^2 - 2b^2$, $q = s^2 - 2t^2$, $\theta = 2^{1/2}$, $\pi = a + b\theta$, $\tau = s + t\theta$; in (viii) and (ix) we set $p = a^2 + 2b^2$, $q = s^2 + 2t^2$, $\theta = (-2)^{1/2}$, $\pi = a + b\theta$, $\tau = s + t\theta$. In all cases, a, b, s, t are positive, and the symbol $(\alpha : \pi)$ denotes the residue ± 1 of $\alpha^{(p-1)/2}$ modulo π in the ring $Z[\theta]$.

(vi) Since $pq = (as + 2bt)^2 - 2(at + bs)^2$, $g((as + 2bt - 1)/2, 1) = (at + bs)^2$. Since d is fundamental, $at + bs$ is prime to d, and $\chi(g) = (at + bs : p)$, which is as good a formula as any for computational purposes. We can show that $\chi(g) = (\tau : \pi)$ as follows: $(at + bs : p) = (at + bs : \pi) = (bs - tb\theta : \pi) = (b : p)(\bar{\tau} : \pi) = (p : b')(\bar{\tau} : \pi)$ where b' is the odd part of b; since $p \equiv a^2 \bmod b'$ and $(\bar{\tau} : \pi)(\tau : \pi) = (q : p) = 1$, $\chi(g) = (\tau : \pi)$.

(vii) Since $pq = 2(as + 2bt + at + bs)^2 - (as + 2bt + 2at + 2bs)^2$

$$\chi(g) = (as + 2bt + 2at + 2bs : p) = (as + 2bt + 2at + 2bs : \pi)$$
$$= (b\theta(-1 + \theta) : \pi)(\bar{\tau} : \pi) = (a + 2b : p)(\bar{\tau} : \pi).$$

Since $(a + 2b)^2 = -p + 2(a + b)^2$, $(a + 2b : p) = (-1 : p)_8$ by Lemma 6. Thus $\chi(g) = (-1 : p)_8(\bar{\tau} : \pi) = (-1 : p)_8(\tau : \pi)$.

(viii) Since $pq = (as - 2bt)^2 + 2(bs + at)^2$, $g((as - 2bt - 1)/2, 1) = (bs + at)^2$, $\chi(g) = (bs + at : p) = (bs + at : \pi) = (bs - bt\theta : \pi) = (b : \pi)(\bar{\tau} : \pi) = (b : p)(\bar{\tau} : \pi) = (\tau : \pi)$ as in (vii).

(ix) Since $(as - 2bt)^2 = -2(bs + at)^2 + pq$, $\chi(g) = (as - 2bt : p) = (as - 2bt : \pi) = (-bs\theta - 2bt : \pi) = (-b\theta : \pi)(\bar{\tau} : \pi) = (a : \pi)(\bar{\tau} : \pi) = (a : p)(\bar{\tau} : \pi)$. Since $p - 2b^2 = a^2$, $(a : p) = (2 : p)_4$ by Lemma 5, and since $(\tau : \pi)(\bar{\tau} : \pi) = (q : p) = 1$, $\chi(g) = (2 : p)_4(\tau : \pi)$.

In what follows, $s^2 \equiv q \bmod p$, $t^2 \equiv q \bmod r$.

For primes p, q of the form $4n + 1$ with $(p : q) = 1$, q is represented by the genus of $[1, 0, -p]$, hence $qx^2 = y^2 - pz^2$ has a solution with

$(y, z) = 1$, x, y, and z positive and x odd. If $a^2 - qb^2 = -1$, a and b positive, then $q(ax + by)^2 - pz^2 = (ya + qbx)^2$. Lemma 5 gives

$$(p : q)_4 = (ya + qbx : q) = (q : ya + qbx) = (p : ya + qbx)$$
$$= (ya + qbx : p) = (\pm sxa + qbx : p) = (\pm sx : p)(a \pm sb : p)$$
$$= (s : p)(p : x)(a \pm sb : p),$$

the sign being $+$ if $y \equiv sx$ and $-$ if $y \equiv -sx$. Since $(s : p) = (q : p)_4$, $pz^2 \equiv y^2 \bmod x$ and $(a + sb : p)(a - sb : p) = (-1 : p) = 1$, we have the following.

COROLLARY 8 [6, 7]. *For primes $p \equiv q \equiv 1 \bmod 4$ with $(p : q) = 1$, $(p : q)_4(q : p)_4 = (a + sb : p)$ where $a^2 - qb^2 = -1$.*

We will also use the familiar property of Gaussian composition that:

LEMMA 9. *If $l = hk$ under a Gaussian bilinear substitution expressing z_1, z_2 in terms of x_1, x_2 and y_1, y_2, and if $(m, n) = 1$, $m = h(x_1, x_2)$, $n = k(y_1, y_2)$, $(x_1, x_2) = 1 = (y_1, y_2)$, then $mn = l(z_1, z_2)$ with $(z_1, z_2) = 1$.*

(x) Since $[-p, 0, q]$ is in the principal genus we can write $-px^2 + qy^2 = z^2$ with x, y, z positive and $(x, y) = 1$, z odd. Since 2 is represented by the principal genus of discriminant $4q$ (in fact, 2 is represented by the principal class) we can write $v^2 - qw^2 = 2u^2$ with u, v, w positive and $(u, px) = 1 = (v, w)$. By composition,

$$(vz + qyw)^2 = q(vy + zw)^2 - 2p(xu)^2, \qquad (vy + zw, xu) = 1.$$

Hence

$$\chi(g) = (vz + qyw : pq) = (v : q)(z : q)(vz + qyw : p)$$
$$= (v : q)(z : q)(\pm syv + qyw : p) = (v : q)(z : q)(\pm sy : p)(v \pm sw : p)$$
$$= (v : q)(z : pq)(v \pm qw : p),$$

the sign being $+$ if $z \equiv sy \bmod p$ and $-$ if $z \equiv -sy \bmod p$. Since $(z : pq) = (pq : z) = 1$ and $(v + sw : p)(v - sw : p) = (2 : p) = 1$, $\chi(g) = (v : q)(v + sw : p)$. By Lemma 6, $\chi(f) = (-1 : pq)_8$.

(xi) Since p and $-r$ are represented by the genus of $[4, 0, -q]$, we can write $px^2 = 4y^2 - qz^2$, $-ru^2 = 4v^2 - qw^2$, with $(x, r) = (u, px) = (y, z) = (v, w) = (xu, 2) = 1$, $x, \ldots, w$ positive. Thus $-pr(xu)^2 = (4yv + qzw)^2 - q(2yw + 2zv)^2$, and $(4yv + qzw)^2$ is prime to $4pq$ and primitively represented by g. Thus

$$\chi(g) = (4yv + qzw : qr) = (2y : q)(2v : q)(\pm 2ywt + qzw : r)$$
$$= (2y : q)(2v : q)(\pm w : r)(2y \pm tz : r)$$
$$= (2y : q)(2v : rq)(2y \pm tz : r).$$

If $rq \equiv 1 \bmod 8$, $(2v : rq) = (v' : rq) = (rq : v') = 1$, v' the odd part of v. If $rq \equiv 5 \bmod 8$, v is odd and $(2v : rq) = (2 : rq)(rq : v) = (2 : rq)$. Since $(2y + tz : r)(2y - tz : r) = (p : r) = 1$, $\chi(g) = (2y : q)(2 : rq)(2y + tz : r) = (y : q)(4y + 2tz : r)$. By Lemma 5, $\chi(f) = (rq : p)_4$.

A connection should be mentioned between our problem and that of the parity of u_1, where t_1, u_1 denotes the least positive solution of $t^2 - du^2 = 4$. By Theorem 1a of [3], if $d \equiv -4 \bmod 16$ (or 0 mod 32), an ambiguous class contains forms (10) of only one type if u_1 is even, but of both types if u_1 is odd. It follows in cases (vi) and (viii) that u_1 is even if and only if I is equivalent to f, and u_1 is odd if and only if I is equivalent to fg or g.

There is a reasonable likelihood that our methods can be adapted to solve the problem of determining the "second form" completely, except when there is more than one ambiguous class in the principal spinor genus. Whether characters can be constructed to meet the needs of spinor genera of higher order remains to be seen.

Acknowledgment

We wish to thank Olga Taussky-Todd, who brought certain recent literature on the representability of -1 to our attention, and then encouraged us to work out the details when, on comparing notes, the two of us surmised that the whole subject was basically a problem of spinor genera.

References

1. G. L. Watson, Integral quadratic forms, Cambridge Univ. Press, 1960.
2. G. Lejeune Dirichlet, Werke I, pp. 65–98, 197–218, and 221–236.
3. G. Pall, Discriminantal divisors of binary quadratic forms, *J. Number Theory*, **1** (1969), 525–533.
4. K. Burde, Ein rationales biquadratisches Reziprozitätsgesetz, *J. Reine Angew. Math.* **235** (1969), 175–184.
5. Ezra Brown, The power of 2 dividing the class number of a binary quadratic discriminant, *J. Number Theory* **5** (1973), 413–419.
6. A. Scholz, Über die Lösbarkeit der Gleichung $t^2 - Du^2 = -4$, *Math. Z.* **39** (1934), 97.
7. E. Lehmer, On the quadratic character of some quadratic surds, *J. Reine Angew. Math.* **250** (1971), 42–48.
8. Daniel Shanks, Gauss's ternary form reduction and the 2-Sylow subgroup, *Math. Comp.* **25** (1971), 837–853.
9. D. Estes and G. Pall, A reconsideration of Legendre-Jacobi symbols, *J. Number Theory* **5** (1973), 433–434.