DISCRIMINANTAL DIVISORS AND BINARY QUADRATIC FORMS

by EZRA BROWN

(Received 20 April, 1970)

1. Introduction. An ancipital form is a form $[a, b, c]$ in which $b = 0$ or $b = a$; these fall into pairs of associates: $[a, 0, c]$ and $[c, 0, a]$ (type 1), and $[a, a, c]$ and $[4c-a, 4c-a, c]$ (type 2). The set of discriminantal divisors of discriminant d is formed by choosing, from each pair of primitive associate ancipital forms of discriminant d, exactly one of the two leading coefficients. In this article we study representations of discriminantal divisors of a given discriminant by binary quadratic forms of that discriminant, previously studied by the author and by G. Pall. We are concerned here with discriminants $d = 4^k pq$, where $k \geqq 1$, $p \equiv 1$, $q \equiv 3 \pmod 4$ are primes, and $d = 4^k p$, where $k \geqq 1$ and p is an odd prime. This investigation arose in connection with the search for integral solutions of $x^2 - Dy^2 = -1$.

2. Preliminary results for the case $d = 4pq$. Suppose that $p \equiv 1$, $q \equiv 3 \pmod 4$. Since $d \equiv -4 \pmod{16}$, there are the generic characters $(f\,|\,p)$, $(f\,|\,q)$, and $(-1\,|\,f)$; hence there are four genera and eight pairs of primitive associate ancipital forms. The eight discriminantal divisors (DD's) associated with these forms turn out to be ± 1, ± 2, $\pm q$, and $\pm 2q$. Now a necessary condition that $f_1 = [1, 0, -pq]$ represent k, a given DD, is that f_1 be in the genus of the ancipital form whose leading coefficient is k. If we construct a table of generic characters for the eight appropriate ancipital forms, we may deduce the following theorem:

THEOREM 1. *Suppose that $f_1 = [1, 0, -pq]$, where $p \equiv 1$, $q \equiv 3 \pmod 4$ are primes.*

(a) *Suppose that $(p\,|\,q) = -1$. Then f_1 represents 2 if $(2\,|\,p) = (2\,|\,q) = 1$, -2 if $(2\,|\,p) = -(2\,|\,q) = 1$, $2q$ if $-(2\,|\,p) = (2\,|\,q) = 1$, and $-2q$ if $(2\,|\,p) = (2\,|\,q) = -1$.*

(b) *Suppose that $(p\,|\,q) = 1$. If $(2\,|\,p) = -1$, then f_1 represents $-q$; if $(2\,|\,p) = 1$, then f_1 represents $\{-q, 2, -2q\}$ or $\{-q, -2, 2q\}$, according as $(2\,|\,q) = 1$ or -1.*

The undecided cases are $(p\,|\,q) = (2\,|\,p) = 1$; so we consider these now. In particular, we take the case $(2\,|\,q) = -1$, and determine necessary conditions that f_1 represent -2, $-q$, or $2q$. The case $(2\,|\,q) = 1$ will be studied later.

THEOREM 2. *Let $(p\,|\,q) = 1$, where $p \equiv 1$, $q \equiv 3 \pmod 8$ are primes; we may then write $q = A^2 + 2B^2$. If $f_1 = [1, 0, -pq]$ represents -2, then there exist integers x_1 odd, x_2 even such that $p = x_1^2 + 2x_2^2$, and either*

(a) $(Ax_2 + Bx_1\,|\,q) = (-1\,|\,Ax_2 + Bx_1) = 1$, *or*

(b) $(Ax_2 - Bx_1\,|\,q) = (-1\,|\,Ax_2 - Bx_1) = 1$.

Proof. Suppose that there exist u, v $(v > 0)$ such that $u^2 - pqv^2 = -2$; then $g = [pqv, 2u, v]$ has determinant 2, and so $g \sim [1, 0, 2]$. Consider the following Cantor diagram (see **[1]**), with $\det T = 1$:

$$[1, 0, 2] \xrightarrow{T} [pqv, 2u, v],$$
$$h = [a, 2b, c] \xleftarrow{T'} [1, 0, -pq].$$

https://doi.org/10.1017/S0017089500001397 Published online by Cambridge University Press

By Proposition 3.3 of [**1**], $a+2c=0$; so there is a form $h=[-2c, 2b, c]\sim f_1$; comparing determinants, we have $pq=b^2+2c^2$. Since $(-2\,|\,p)=(-2\,|\,q)=1$, and p, q are primes, there exist x_1 odd, x_2 even, A odd, B odd (unique up to choice of sign) such that $p=x_1^2+2x_2^2$ and $q=A^2+2B^2$. Hence $pq=(Ax_1\pm 2Bx_2)^2+2(Ax_2\mp Bx_1)^2=b^2+2c^2$. Since h is in the genus of f_1, $(-1\,|\,c)=(c\,|\,q)=1$ (c is odd, since h is primitive). From this the conclusion follows.

THEOREM 3. *Let $p\equiv 1$, $q\equiv 3 \pmod 8$ be primes. Suppose that the only classes of determinant $-2q$ are represented by $\pm[1, 0, -2q]$. If f_1 represents $2q$, then there exist x_3, x_4 both odd such that $p=qx_4^2-2x_3^2$ and $(x_3\,|\,q)=(-1\,|\,x_3)=1$.*

Proof. If there exist u, v such that $u^2-pqv^2=2q$, then $g=[pqv, 2u, v]$ has determinant $-2q$; by hypothesis, $g\sim[1, 0, -2q]$ or $g\sim[-1, 0, 2q]$. In either case, we have the following Cantor diagram ($\det T=1$):

$$[\pm 1, 0, \mp 2q]\xrightarrow{T}[pqv, 2u, v],$$

$$[a, 2b, x_3]\xleftarrow{T'}[1, 0, -pq].$$

By Proposition 3.3 of [**1**], $a=2qx_3$; so there is a form $h=[2qx_3, 2b, x_3]\sim f_1$; comparing determinants, we have $pq=b^2-2qx_3^2$. Hence $b=qx_4$, $p=qx_4^2-2x_3^2$; since h is primitive and pq is odd, x_3 and x_4 are both odd, and since h is in the genus of f_1, $(-1\,|\,x_3)=(x_3\,|\,q)=1$.

REMARK. The hypothesis that there be only two classes of determinant $-2q$ is not strong; the smallest prime $q\equiv 3 \pmod 8$ not having this property is 163.

As in the case $p\equiv q \pmod 4$, the necessary conditions that f_1 represent $-q$ depend upon the class number $h(q)$ of determinant q; if $h(q)$ is large, these necessary conditions may be complicated. However, we may prove the following general theorem.

THEOREM 4. *Let $p\equiv 1$, $q\equiv 3 \pmod 8$ be primes, and suppose that $u^2-pqv^2=-q$. Let $g=[pqv, 2u, v]$ and $g_1=[1, 0, q]$. If $g\sim g_1$, then there exist x_5 odd, x_6 even such that $p=x_5^2+qx_6^2$, and $(x_5\,|\,q)=(-1\,|\,x_5)=1$.*

Proof. The result follows from the Cantor diagram ($\det T=1$):

$$[1, 0, q]\xrightarrow{T}[pqv, 2u, v],$$

$$h=[a, 2b, x_5]\xleftarrow{T'}[1, 0, -pq].$$

As in [**1**], we find it useful to study a system of diophantine equations in order to discern any relationships among the forms discussed in Theorems 2, 3, and 4. We study the system

$$p=x_1^2+2x_2^2=qx_4^2-2x_3^2=x_5^2+qx_6^2 \tag{1}$$

in the case x_1, x_3, x_4, x_5 odd, x_2, x_6 even, $p\equiv 1 \pmod 8$ and $q\equiv 3 \pmod 8$ primes, and p representable by $x_1^2+2x_2^2$ and $x_5^2+qx_6^2$.

First, we study the solutions of

$$x_1^2+2x_2^2=qx_4^2-2x_3^2 \tag{2}$$

in the above case. We see that $Q=x_1 i_1+x_2 i_2+x_3 i_3$ is an element of norm qx_4^2 in the ring of generalized quaternions with multiplication $i_1^2 = -1$, $i_2^2 = i_3^2 = i_1 i_2 i_3 = -2$. The norm form of this ring, $x^2+y^2+2z^2+2w^2$, is in a genus of one class (see [3]); as a consequence of this and Theorem 3 of [3] we may write $Q = \bar{\sigma}\tau\sigma$, where $N(\tau) = q$, $N(\sigma) = x_4$, and σ and τ are unique up to multiplication by unit factors (see [1] for elaboration). Since q is a prime $\equiv 3 \pmod 8$, there exist A, B, both odd, such that $q = A^2+2B^2$, where A and B are unique up to choice of sign. It is not hard to show that, if $\tau = ai_1+bi_2+ci_3$, then $a \equiv x_1$, $b \equiv x_2$ and $c \equiv x_3 \pmod 2$; hence the only possibilities for τ are $\pm(Ai_1 \pm Bi_3)$. If we use $\tau_1 = Ai_1+Bi_3$, write $\sigma = s_0+s_1 i_1+s_2 i_2+s_3 i_3$, and expand $\bar{\sigma}\tau_1\sigma$, we obtain the following expressions:

$$\left.\begin{aligned} x_1 &= A(s_0^2+s_1^2-2s_2^2-2s_3^2)+4B(-s_0 s_2+s_1 s_3), \\ x_2 &= 2A(-s_0 s_3+s_1 s_2)+2B(s_0 s_1+2s_2 s_3), \\ x_3 &= 2A(s_0 s_2+s_1 s_3)+B(s_0^2+2s_3^2-s_1^2-2s_2^2), \\ x_4 &= s_0^2+s_1^2+2s_2^2+2s_3^2 \qquad (\text{where } s_0 \not\equiv s_1 \pmod 2). \end{aligned}\right\} \tag{3}$$

It is straightforward to show that, if we replace τ_1 by one of the other three eligible τ's, we gain no new solutions; hence all parametric solutions of (2) are given by the expressions (3).

Consider the following expressions for x_5 and x_6, obtained by considering special cases:

$$\left.\begin{aligned} x_5 &= A(s_0^2+2s_3^2-s_1^2-2s_2^2)+4B(-s_0 s_2-s_1 s_3), \\ x_6 &= 2(s_0 s_1-2s_2 s_3). \end{aligned}\right\} \tag{4}$$

The expressions in (3) and (4), when substituted into the following equations, yield an identity:

$$x_1^2+2x_2^2 = qx_4^2-2x_3^2 = x_5^2+qx_6^2. \tag{5}$$

Since the expressions in (3) yield all solutions of (2), and since the representations of a prime by the forms $x_1^2+2x_2^2$ and $x_5^2+qx_6^2$ (q a prime) are essentially unique, it follows that all solutions of (1) in the stated case are given by the parametric expressions for $x_1, \ldots, x_6$ in (3) and (4). The key to the solution of this system is that the norm-form $x^2+y^2+2z^2+2w^2$ is in a genus of one class; hence the factorization of Q as $\bar{\sigma}\tau\sigma$ given above is essentially unique.

3. The main theorem, for $q = 3$. First, we prove

THEOREM 5. *Suppose that* $p \equiv 1 \pmod 8$, $(p\,|\,3) = 1$, *and* $f_1 = [1, 0, -3p]$. *If* f_1 *represents* -3, *then* (a) *there exist* x_5 *odd,* x_6 *even such that* $p = x_5^2+3x_6^2$. *Furthermore,* (b) $x_5 \equiv \pm 1 \pmod 6$ *and* $x_6 \equiv 0 \pmod 4$.

Proof. Let $u^2-3pv^2 = -3$; then $g = [3pv, 2u, v]$ has determinant 3. If $g \sim [1, 0, 3]$, then (a) is true by Theorem 4. If $g \sim [2, 2, 2]$ (the only other possibility), we deduce that there is a form $h = [-b-c, 2b, c] \sim f_1$, by examining the following Cantor diagram, in which $\det T = 1$:

$$[2, 2, 2] \xrightarrow{T} [3pv, 2u, v],$$

$$h = [a, 2b, c] \xleftarrow{T'} [1, 0, -3p].$$

https://doi.org/10.1017/S0017089500001397 Published online by Cambridge University Press

Hence $3p = b^2+bc+c^2$; one of b, c is odd; so we suppose in view of the symmetry that b is odd. We may assume that c is even, for if c is also odd, we can replace c by $b+c$ and b by $-b$. Writing $c = 2x_5$, we obtain $3p = (b+x_5)^2+3x_5^2$; writing $b+x_5 = 3x_6$, we obtain $p = x_5^2+3x_6^2$. By hypothesis, $p \equiv 1 \pmod{24}$, so we must have x_5 odd and x_6 even. To prove (b) in either case, we observe that $(p, 3) = 1$ and so $x_5 \equiv \pm 1 \pmod 6$; hence $x_5^2 \equiv 1 \pmod{24}$ and so $x_6 \equiv 0 \pmod 4$.

Now we may prove

THEOREM 6. *Let* $p \equiv 1 \pmod 8$, $(p\,|\,3) = 1$, $f_1 = [1, 0, -3p]$, *and let* $x_1, \ldots, x_6$ *be as in equation* (1).

(a) *If* $x_5 \equiv \pm 5 \pmod{12}$, *then* f_1 *never represents* -3; *it represents* 6 *or* -2, *according as* $\pm x_3 \equiv 1$ *or* 5 (mod 12), *or equivalently, according as* $\pm(x_1+x_2) \equiv 5$ *or* 1 (mod 12).

(b) *If* $x_5 \equiv \pm 1 \pmod{12}$, *then* f_1 *represents* -3 *if* $\pm x_3 \equiv 5 \pmod{12}$; *otherwise, any of* -2, -3, *or* 6 *may be represented.*

The proof is based on the following lemma. Here, $x_1, \ldots, x_6, s_0, \ldots, s_3$ are as in (3) and (4).

LEMMA 6.1. (a) *If* $x_5 \equiv \pm 5 \pmod{12}$, *then* $x_3 \equiv \pm 1 \pmod{12}$ *if and only if* $x_1+x_2 \equiv \pm 5 \pmod{12}$.

(b) *If* $x_5 \equiv \pm 1 \pmod{12}$, *then* $\pm x_3 \equiv x_1+x_2 \pmod{12}$.

Proof. We shall prove (a) in the case $s_2 \equiv s_3 \pmod 2$. The proofs for the case $s_2 \not\equiv s_3 \pmod 2$ and for (b) are similar.

Assume that $s_2 \equiv s_3 \pmod 2$. We observe that $x_5 \equiv (s_0-2s_2)^2-(s_1+2s_3)^2 \pmod{12}$. If $x_5 \equiv \pm 5 \pmod{12}$, then either (i) $s_0-2s_2 \equiv \pm 2$, $s_1+2s_3 \equiv 3 \pmod 6$, or (ii) $s_0-2s_2 \equiv 3$, $s_1+2s_3 \equiv \pm 2 \pmod 6$. Similarly, we observe that, if $x_3 \equiv \pm 1 \pmod{12}$, then either (i) $s_0+s_2 \equiv \pm 1$, $s_1-s_3 \equiv 0 \pmod 6$, or (ii) $s_0+s_2 \equiv 0$, $s_1-s_3 \equiv \pm 1 \pmod 6$. Then we observe that $\pm(x_1+x_2) \equiv ((s_0-2s_2)+(s_1+2s_3))^2+6(s_0s_3+s_1s_2) \pmod{12}$, so that $x_1+x_2 \equiv \pm 5 \pmod{12}$ implies that $s_0s_3+s_1s_2$ is odd and $(s_0-2s_2)+(s_1+2s_3) \equiv \pm 1 \pmod 6$. Finally, if $x_5 \equiv \pm 5 \pmod{12}$, we observe that (i) $s_0 \not\equiv s_1$, $s_2 \equiv s_3 \equiv 1 \pmod 2$, (ii) $x_3 \equiv \pm 1 \pmod{12}$, and (iii) $x_1+x_2 \equiv \pm 5 \pmod{12}$ are equivalent statements. This proves (a) in the case $s_2 \equiv s_3 \pmod 2$.

Proof of the theorem. (a) If $x_5 \equiv \pm 5 \pmod{12}$, the necessary conditions of Theorem 5 for f_1 to represent -3 are violated; hence f_1 does not represent -3. By the lemma, the conditions of Theorem 2 for f_1 to represent -2 are violated if $x_3 \equiv \pm 1 \pmod{12}$, and those of Theorem 3 for f_1 to represent 6 are violated if $x_3 \equiv \pm 5 \pmod{12}$. This proves (a).

(b) If $x_5 \equiv \pm 1 \pmod{12}$, and $x_3 \equiv \pm 5 \pmod{12}$, then, by the lemma and Theorems 2 and 3, f_1 represents neither -2 nor 6; hence f_1 represents -3. If $x_3 \equiv \pm 1 \pmod{12}$, the following are examples demonstrating the latter statement of (b): $[1, 0, -3p]$ represents -2, -3, and 6, respectively, when $p = 937$, 433, and 673, respectively.

4. The cases $d = 4^kpq$ and $d = 4^kp$ ($k \geq 1$).

THEOREM 7. *Let* $p \equiv 1$, $q \equiv 3 \pmod 8$ *be primes*; *let* $f_k = [1, 0, -4^{k-1}pq]$ *be the principal form of discriminant* 4^kpq.

https://doi.org/10.1017/S0017089500001397 Published online by Cambridge University Press

(a) *If* f_1 *represents any of* $2, -2, 2q$, *or* $-2q$, *or if* $(p\,|\,q) = -1$, *then* f_k *represents* 4^{k-1}, *where* $k \geqq 2$.

(b) *Let* $u^2 - pqv^2$ *be a primitive representation of* $-q$, *and write* $v = 2^m v_0$, *where* v_0 *is odd. Let* $k \geqq 2$. *Then* f_k *represents* $-4^{k-1}q$ *if* $m = 0$, 4 *if* $0 < m < k-3$, $-4q$ *if* $m = k-2$, *and* $-q$ *if* $m \geqq k-1$.

Proof. By examining tables of generic characters, we find that, for $d = 16pq$, the DD's that f_2 may represent are $-q, 4$, and $-4q$, and for $d = 4^k pq$ $(k \geqq 3)$ those that f_k may represent are $-q$, 4, $-4q$, 4^{k-1}, and $-4^{k-1}q$.

Suppose that f_2 represents $-q$; for some u, v with $(u, v) = 1$, we have $u^2 - 4pqv^2 = -q$. Hence u is odd, and $u^2 - pq(2v)^2 = -q$ is a primitive representation of $-q$ by f_1. Similarly, if f_2 represents $-4q$, then f_1 represents $-q$ with u even. Hence, if f_1 represents any of ± 2, $\pm 2q$ (which happens if $(p\,|\,q) = 1$, by Theorem 1), then f_2 represents neither $-q$ nor $-4q$, and hence represents 4. If there exist u, v with $(u, v) = 1$, such that $u^2 - 4pqv^2 = 4$, then u is even; so $(2^{k-2}u)^2 - 4^{k-1}pqv^2 = 4^{k-1}$ is a primitive representation of 4^{k-1} by f_k $(k \geqq 3)$, which proves (a).

Suppose that $u^2 - pqv^2 = -q$, with $(u, v) = 1$. Write $v = 2^m v_0$, where v_0 is odd. If $m \geqq k-1$, then $u^2 - 4^{k-1}pq\ (2^{m-k+1}v_0)^2 = -q$, with $(u, 2^{m-k+1}v_0) = 1$. If $m = k-2$, then $u^2 - 4^{k-2}pqv_0^2 = -q$, with u odd, and $(u, v_0) = 1$; so $(2u)^2 - 4^{k-1}pqv_0^2 = -4q$, with $(2u, v_0) = 1$. If $m = 0$, then $(2^{k-1}u)^2 - 4^{k-1}pqv_0^2 = -4^{k-1}q$, with $(2^{k-1}u, v_0) = 1$. Conversely, if f_k represents $-q$, $-4q$, or $-4^{k-1}q$, then $u^2 - pq(2^m v_0)^2 = -q$, with $m \geqq k-1$, $m = k-2$, or $m = 0$, respectively. Hence $0 < m < k-3$ implies that f_k represents 4, which proves (b).

Using the same techniques, we prove

THEOREM 8. *Let* p *be an odd prime. Let* $g_k = [1, 0, -4^{k-1}p]$, *where* $k \geqq 2$. *Then* g_k *represents* -4^{k-1} *or* 4^{k-1}, *according as* $p \equiv 1$ *or* $3 \pmod 4$. *Also*, $[1, 0, -p]$ *represents* -1 *if* $p \equiv 1 \pmod 4$, -2 *if* $p \equiv 3 \pmod 8$, *and* 2 *if* $p \equiv 7 \pmod 8$.

The proof is immediate if one realizes that the discriminant $4p$ has one or two primitive genera, according as $p \equiv 1$ or $3 \pmod 4$, and that, in any case, $[1, 0, -4p]$ must represent 4.

REFERENCES

1. Ezra Brown, Representations of discriminantal divisors by binary quadratic forms, *J. Number Theory* **3** (1971), 213–225.

2. Gordon Pall, On generalized quaternions, *Trans. Amer. Math. Soc.* **59** (1946), 280–332.

3. Gordon Pall, Discriminantal divisors of binary quadratic forms, *J. Number Theory* **1** (1969), 525–532.

VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY
BLACKSBURG, VIRGINIA 24061