

# FORMS REPRESENTABLE BY AN INTEGRAL POSITIVE-DEFINITE BINARY QUADRATIC FORM

KENNETH S. WILLIAMS

## 1. Introduction.

Let  $g(X, Y) = lX^2 + mXY + nY^2$  be an integral, positive-definite, binary quadratic form of discriminant  $-D$ , so that  $l > 0$ ,  $n > 0$ , and  $D = 4ln - m^2 > 0$ . Thus  $D \equiv 0$  or  $3 \pmod{4}$  and we let

$$\begin{aligned} D_1 &= \frac{1}{4}D & , & \text{ if } D \equiv 0 \pmod{4} , \\ &= \frac{1}{4}(D+1) & , & \text{ if } D \equiv 3 \pmod{4} . \end{aligned}$$

We say that a binary quadratic form  $f(X, Y) = aX^2 + bXY + cY^2$  is representable by  $g(X, Y)$  if there exist integers  $a_1, a_2, b_1, b_2$  with  $a_1b_2 - a_2b_1 \neq 0$  such that

$$f(X, Y) = g(a_1X + b_1Y, a_2X + b_2Y) .$$

We are interested in giving necessary and sufficient conditions for a binary quadratic form  $f(X, Y)$  to be representable by  $g(X, Y)$ . Clearly any such  $f(X, Y)$  must be integral and positive-definite, with

$$\begin{aligned} \text{discrim}(f(X, Y)) &= \text{discrim}(g(a_1X + b_1Y, a_2X + b_2Y)) \\ &= (a_1b_2 - a_2b_1)^2 \text{discrim}(g(X, Y)) = -Dk^2 , \end{aligned}$$

where  $k$  is a non-zero integer. Throughout this paper it will be assumed that  $f(X, Y)$  satisfies these conditions. If  $f(X, Y)$  is representable by  $g(X, Y)$ , then  $f(X, Y)$  is representable by any binary quadratic form (properly or improperly) equivalent to  $g(X, Y)$ . Conversely, if  $f(X, Y)$  is representable by some binary quadratic form equivalent to  $g(X, Y)$ , then  $f(X, Y)$  is representable by  $g(X, Y)$ . Now the class of forms equivalent to  $g(X, Y)$  contains one and only one reduced form. Thus, without any loss of generality, we can suppose that  $g(X, Y)$  is reduced, that is,  $l, m, n$ , satisfy  $-l < m \leq l$ ,  $n \geq l$ , with  $m \geq 0$  if  $l = n$ . It is known that there is only a finite number of integral, positive-definite, reduced forms with discriminant  $-D$ . We make the assumption throughout this paper that this number is exactly one. From the classical work of Gauss and a recent result of Stark [5] we know that this occurs precisely for

$$(1.1) \quad D = 3, 4, 7, 8, 11, 19, 43, 67, 163 .$$

In this case the single reduced form is the principal form so that we have

$$g(X, Y) \equiv g_D(X, Y) = \begin{cases} X^2 + D_1 Y^2 & , \quad \text{if } D \equiv 0 \pmod{4} , \\ X^2 + XY + D_1 Y^2 & , \quad \text{if } D \equiv 3 \pmod{4} . \end{cases}$$

When  $D = 4$  representability of  $f(X, Y) = aX^2 + bXY + cY^2$  by  $g_4(X, Y) = X^2 + Y^2$  has been considered by Mordell [2]. (An omission in his proof has been corrected by Niven [3].) If we write  $r_D(h)$  for the number of representations of the positive integer  $h$  by any integral, positive-definite, binary quadratic form of discriminant  $-D$  (equivalently the number of ordered pairs of integers  $(u, v)$  such that  $h = g_D(u, v)$ ), we can state Mordell's theorem as follows:

**THEOREM (Mordell).** *Let  $f(X, Y) = aX^2 + bXY + cY^2$  be an integral, positive-definite, binary quadratic form of discriminant  $-4k^2$ , where  $k$  is a non-zero integer, so that  $b$  is an even integer. Then  $f(X, Y)$  is representable by any integral, positive-definite, binary quadratic form of discriminant  $-D$ , if and only if  $r_4(d) > 0$ , where, here and throughout this paper,  $d = \text{G.C.D.}(a, b, c)$ .*

In Section 2 we determine the value of  $r_D(h)$  for all  $D$  given by (1.1). In Section 3 we prove two lemmas which are used in Section 4, where we prove the following generalization of Mordell's theorem.

**THEOREM 1.** *Let  $f(X, Y) = aX^2 + bXY + cY^2$  be an integral, positive-definite, binary quadratic form of discriminant  $-Dk^2$ , where  $k$  is a non-zero integer and  $D$  is given by (1.1). Then  $f(X, Y)$  is representable by any integral, positive-definite, binary quadratic form of discriminant  $-D$  if and only if  $r_D(d) > 0$ .*

As regards the number of representations of  $f(X, Y)$  by a form of discriminant  $-D$ , Pall [4] has proved the following theorem for the case  $D = 4$ .

**THEOREM (Pall).** *Let  $f(X, Y) = aX^2 + bXY + cY^2$  be an integral, positive-definite, binary quadratic form of discriminant  $-4k^2$ , where  $k$  is a non-zero integer. Then the number of representations of  $f(X, Y)$  by any integral, positive-definite, binary quadratic form of discriminant  $-4$  is  $2r_4(d)$ .*

In Section 5 we generalize this result by proving the following:

**THEOREM 2.** *Let  $f(X, Y) = aX^2 + bXY + cY^2$  be an integral, positive-definite, binary quadratic form of discriminant  $-Dk^2$ , where  $k$  is a non-*

zero integer and  $D$  is given by (1.1). Then the number of representations of  $f(X, Y)$  by any integral, positive-definite, binary quadratic form of discriminant  $-D$  is  $2r_D(d)$ .

We remark that our proof of theorem 2 is much simpler than the one given by Pall [4] for the case  $D=4$ .

We conclude this introduction by noting that we write, throughout this paper,  $p(D)$  for the unique prime dividing  $D$ , where  $D$  is given by (1.1), so that

$$p(D) = 2, \quad \text{if } D=4, 8, \\ = D, \quad \text{if } D=3, 7, 11, 19, 43, 67, 163.$$

**2. The value of  $r_D(h)$ .**

We calculate the value of  $r_D(h)$ , for  $h$  a positive integer and  $D=3, 4, 7, 8, 11, 19, 43, 67, 163$ , from an old result of Dirichlet (see for example [1]). We shall use the Kronecker symbol  $(\cdot/\cdot)$ .

**THEOREM (Dirichlet).** For  $D=3, 4, 7, 8, 11, 19, 43, 67, 163$  we let

$$w_D = 2, \quad \text{if } D=7, 8, 11, 19, 43, 67, 163, \\ = 4, \quad \text{if } D=4, \\ = 6, \quad \text{if } D=3,$$

and set

$$(2.1) \quad h = p(D)^\alpha 2^{\alpha_0} p_1^{\alpha_1} \dots p_r^{\alpha_r} q_1^{\beta_1} \dots q_s^{\beta_s},$$

where the  $p_i$  are  $r (\geq 0)$  distinct odd primes  $\neq p(D)$  such that  $(-D/p_i) = +1$ ; the  $q_j$  are  $s (\geq 0)$  distinct odd primes  $\neq p(D)$  such that  $(-D/q_j) = -1$ ;  $\alpha_i > 0, i=1, \dots, r; \beta_j > 0, j=1, \dots, s; \alpha \geq 0; \alpha_0 \geq 0$  with  $\alpha_0=0$  if  $D=4$  or 8. Then

$$(2.2) \quad \left\{ \begin{array}{l} r_D(h) = w_D \prod_{i=0}^r (\alpha_i + 1) \prod_{j=1}^s \frac{1}{2} (1 + (-1)^{\beta_j}), \\ \text{if } D=4, 7 \text{ or } 8, \text{ and} \\ r_D(h) = w_D \frac{1}{2} (1 + (-1)^{\alpha_0}) \prod_{i=1}^r (\alpha_i + 1) \prod_{j=1}^s \frac{1}{2} (1 + (-1)^{\beta_j}), \\ \text{if } D=3, 11, 19, 43, 67, 163. \end{array} \right.$$

**PROOF.** We begin by showing that for any positive integer  $k$  we have

$$(2.3) \quad r_D(p(D)k) = r_D(k).$$

We set

$$S_D(k) = \{(x, y) \mid x, y \text{ integers with } g_D(x, y) = k\}.$$

If  $D=4$  (so that  $p(D)=2$ ) the mapping  $\lambda : S_4(2k) \rightarrow S_4(k)$  defined by

$$\lambda((x, y)) = (\frac{1}{2}(x+y), \frac{1}{2}(x-y))$$

is a bijection, so that  $|S_4(2k)| = |S_4(k)|$ , that is,  $r_4(2k) = r_4(k)$ . If  $D = 8$  (so that  $p(D) = 2$ ), the mapping  $\lambda : S_8(2k) \rightarrow S_8(k)$  defined by

$$\lambda((x, y)) = (y, \frac{1}{2}x)$$

is a bijection, so that  $|S_8(2k)| = |S_8(k)|$ , that is,  $r_8(2k) = r_8(k)$ . For  $D \neq 4$  or 8 (so that  $p(D) = D$ ) the mapping  $\lambda : S_D(Dk) \rightarrow S_D(k)$  defined by

$$\lambda((x, y)) = \left( \frac{-2x + (D-1)y}{2D}, \frac{2x + y}{D} \right)$$

is a bijection, so that  $|S_D(Dk)| = |S_D(k)|$ , that is,  $r_D(Dk) = r_D(k)$ . Thus for all  $D$  we have (2.3). Hence from (2.1) and (2.3) we have  $r_D(h) = r_D(h_1)$ , where

$$h_1 = 2^{\alpha_0} p_1^{\alpha_1} \dots p_r^{\alpha_r} q_1^{\beta_1} \dots q_s^{\beta_s} \quad \text{and} \quad \text{G.C.D.}(h_1, D) = 1,$$

recalling that  $\alpha_0 = 0$  when  $D = 4$  or 8. Now, for  $D = 3, 4, 7, 8, 11, 19, 43, 67, 163$  the class number of discriminant  $-D$  is one, so that by a theorem of Dirichlet [1] we have

$$r_D(h_1) = w_D \sum_{e|h_1} (-D/e).$$

Since the Kronecker symbol  $(-D/e)$  is (completely) multiplicative with respect to  $e$ ,  $\sum_{e|h_1} (-D/e)$  is multiplicative with respect to  $h_1$ , and we have

$$r_D(h) = w_D \left\{ \sum_{e|2^{\alpha_0}} (-D/e) \right\} \left\{ \prod_{i=1}^r \left( \sum_{e|p_i^{\alpha_i}} (-D/e) \right) \right\} \left\{ \prod_{j=1}^s \left( \sum_{e|q_j^{\beta_j}} (-D/e) \right) \right\}.$$

Now as

$$\begin{aligned} (-D/2) &= +1, & \text{if } D = 7, \\ &= 0, & \text{if } D = 4, 8, \\ &= -1, & \text{if } D = 3, 11, 19, 43, 67, 163, \end{aligned}$$

we have

$$\begin{aligned} \sum_{e|2^{\alpha_0}} (-D/e) &= \sum_{l=0}^{\alpha_0} (-D/2^l) = \sum_{l=0}^{\alpha_0} (-D/2)^l \\ &= \begin{cases} \alpha_0 + 1, & \text{if } D = 4, 7, 8, \\ \frac{1}{2}(1 + (-1)^{\alpha_0}), & \text{if } D = 3, 11, 19, 43, 67, 163. \end{cases} \end{aligned}$$

Also for  $i = 1, \dots, r$  we have

$$\sum_{e|p_i^{\alpha_i}} (-D/e) = \sum_{l=0}^{\alpha_i} (-D/p_i^l) = \sum_{l=0}^{\alpha_i} (-D/p_i)^l = \alpha_i + 1,$$

and for  $j = 1, \dots, s$  we have

$$\sum_{e|q_j^{\beta_j}} (-D/e) = \sum_{l=0}^{\beta_j} (-D/q_j^l) = \sum_{l=0}^{\beta_j} (-D/q_j)^l = \frac{1}{2}(1 + (-1)^{\beta_j}).$$

This completes the proof of (2.2).

As immediate consequences of Dirichlet's theorem we have:

**COROLLARY 1.** *If  $h$  is a positive integer then  $r_D(h) = 0$  if and only if there exists some prime  $q$  (possibly  $q = 2$  if  $D = 3, 11, 19, 43, 67$  or  $163$ ) with  $(-D/q) = -1$ , which divides  $h$  to an odd power.*

**COROLLARY 2.** *If  $h$  is a positive integer then  $r_D(h) > 0$  if and only if every prime  $q|h$ , with  $(-D/q) = -1$ , divides  $h$  to an even power.*

**3. Two lemmas.**

In this section we prove two lemmas which will be needed in the proof of theorem 1.

**LEMMA 1.** *Let  $q$  be a prime such that  $(-D/q) = -1$ , where  $D$  is given by (1.1). If  $k$  is a non-negative integer and  $x, y$  integers such that  $q^k | g_D(x, y)$ , then  $q^{k_1} | x$  and  $q^{k_1} | y$ , where  $k_1 = [\frac{1}{2}(k + 1)]$ .*

**PROOF.** If  $k = 0$  the result is trivial so we can suppose  $k \geq 1$ . We consider three cases.

*Case (i).*  $q \neq 2, D = 4$  or  $8$ .

As  $q \neq 2$  we have  $(-D_1/q) = (-4D_1/q) = (-D/q) = 1$ . Now  $q^k | x^2 + D_1y^2$  and so as  $k \geq 1$  we have  $q | x^2 + D_1y^2$ . If  $q | y$  there exists an integer  $z$  such that  $yz \equiv 1 \pmod{q}$  and so  $(xz)^2 \equiv -D_1 \pmod{q}$ , which contradicts  $(-D_1/q) = -1$ . Hence we have  $q | x$ , say  $x = qx_1, y = qy_1$ . Moreover we have  $q^k | q^2(x_1^2 + D_1y_1^2)$  and so if  $k \geq 2, q^{k-2} | x_1^2 + D_1y_1^2$ . If  $k \geq 3$  we can continue in this way obtaining successively

$$\begin{aligned} x_1 &= qx_2, & y_1 &= qy_2, & q^{k-4} &| x_2^2 + D_1y_2^2; \\ x_2 &= qx_3, & y_2 &= qy_3, & q^{k-6} &| x_3^2 + D_1y_3^2; \\ & \dots & & & & \dots; \\ x_{[\frac{1}{2}k]-1} &= qx_{[\frac{1}{2}k]}, & y_{[\frac{1}{2}k]-1} &= qy_{[\frac{1}{2}k]}, & q^{k-2[\frac{1}{2}k]} &| x_{[\frac{1}{2}k]}^2 + D_1y_{[\frac{1}{2}k]}^2. \end{aligned}$$

If  $k$  is even the procedure terminates at this step and we have

$$x = q^{[\frac{1}{2}k]}x_{[\frac{1}{2}k]}, \quad y = q^{[\frac{1}{2}k]}y_{[\frac{1}{2}k]},$$

that is,  $q^{k_1} | x, q^{k_1} | y$ . If  $k$  is odd we can do one more step and obtain

$$x_{[\frac{1}{2}k]} = qx_{[\frac{1}{2}k]+1}, \quad y_{[\frac{1}{2}k]} = qy_{[\frac{1}{2}k]+1},$$

that is,

$$x = q^{[\frac{1}{2}k]+1}x_{[\frac{1}{2}k]+1}, \quad y = q^{[\frac{1}{2}k]+1}y_{[\frac{1}{2}k]+1},$$

or  $q^{k_1} | x, q^{k_1} | y$ .

*Case (ii).*  $q \neq 2, D = 3, 7, 11, 19, 43, 67, 163$ .

Now  $q^k | x^2 + xy + D_1y^2$  and so we have  $q^k | (2x + y)^2 + Dy^2$ . If  $q \nmid y$  there exists an integer  $z$  such that  $yz \equiv 1 \pmod{q}$  and so  $\{(2x + y)z\}^2 \equiv -D \pmod{q}$ ,

which contradicts  $(-D/q) = -1$ . Hence  $q|y$  and so we have  $q|x$ , say  $x=qx_1$ ,  $y=qy_1$ . Moreover if  $k \geq 2$  we have  $q^{k-2}|x_1^2+x_1y_1+D_1y_1^2$ . The proof can now be completed in a similar way to case (i).

*Case (iii).*  $q=2$ .

As  $(-D/2) = -1$  we must have  $D=3, 11, 19, 43, 67, 163$ , and so  $g_D(x, y) = x^2 + xy + D_1y^2$ , where  $D_1 = \frac{1}{2}(D+1)$  is an odd integer. Now  $2^k|x^2+xy+D_1y^2$  so that we have  $2|x^2+xy+y^2$ . If  $2 \nmid y$  then  $2|x^2+x+1$ , which is impossible as  $2|x^2+x$ . Hence  $2|y$  and so we have  $2|x$ , say  $x=2x_1$ ,  $y=2y_1$ . Moreover if  $k \geq 2$  we have  $2^{k-2}|x_1^2+x_1y_1+D_1y_1^2$ , and again the proof can be completed as in cases (i) and (ii).

This completes the proof of lemma 1.

**LEMMA 2.** *Let  $f(X, Y) = aX^2 + bXY + cY^2$  be an integral, positive-definite, binary quadratic form of discriminant  $-Dk^2$ , where  $D$  is given by (1.1) and  $k$  is a non-zero integer. Then  $f'(X, Y) = d^{-1}f(X, Y)$ , where  $d = \text{G.C.D.}(a, b, c)$ , is a primitive, positive-definite, binary quadratic form of discriminant  $-Dk'^2$ , where  $k'$  is a non-zero integer.*

**PROOF.** Clearly  $f'(X, Y)$  is a primitive, positive-definite binary quadratic form. Further, if it has discriminant  $-Dk'^2$ , where  $k'$  is an integer, then it is clear that  $k'$  must be non-zero. Hence it suffices to show that the discriminant of  $f'(X, Y)$  is of the form  $-Dk'^2$ , for some integer  $k'$ . But the discriminant of  $f'(X, Y)$  is the integer  $-Dk^2/d^2$ , so that it suffices to prove that  $d|k$ . If  $D=3, 7, 11, 19, 43, 67, 163$ , this is clear, as in this case  $D$  is prime, and so  $d^2|Dk^2$  implies  $d|k$ . This leaves the cases  $D=4$  and  $D=8$ . We let  $d=2^\alpha d_1$ , where  $\alpha \geq 0$  and  $d_1$  is odd. From  $b^2 - 4ac = -Dk^2$  we deduce that  $b$  must be even, say  $b=2e$ . Thus we have  $ac = e^2 + D_1k^2$ . Now  $2^\alpha|d$  so that  $2^{2\alpha}|ac = e^2 + D_1k^2$ , which implies that  $2^\alpha|e$  and  $2^\alpha|k$ , since  $D_1=1$  or  $2$ . Thus the discriminant of  $f'(X, Y)$  is the integer  $-Dk_1^2/d_1^2$ , where  $k=2^\alpha k_1$ . But  $d_1$  is odd so that as  $D=4$  or  $8$  we must have  $d_1|k_1$ , say  $k_1=d_1k'$ . Then the discriminant of  $f'(X, Y)$  is  $-Dk'^2$ , as required.

#### 4. Necessary and sufficient conditions for representability.

This section is devoted to proving theorem 1. Since all positive-definite, binary quadratic forms of discriminant  $-D$  are equivalent for  $D=3, 4, 7, 8, 11, 19, 43, 67, 163$ , it suffices to show that  $f(X, Y)$  is representable by  $g_D(X, Y)$  if and only if  $r_D(d) > 0$ .

We begin by showing that if  $f(X, Y)$  is representable by  $g_D(X, Y)$  then  $r_D(d) > 0$ . For suppose not, that is  $r_D(d) = 0$ . Then by corollary 1 there exists a prime  $q$ , with  $(-D/q) = -1$ , which divides  $d$  to an odd power,

say  $q^{2s+1} \parallel d$ . Thus we have  $q^{2s+1} | a, q^{2s+1} | b, q^{2s+1} | c$ . Now as  $f(X, Y)$  is representable by  $g_D(X, Y)$ , there exist integers  $a_1, a_2, b_1, b_2$  with  $a_1 b_2 - a_2 b_1 \neq 0$  and such that

$$(4.1) \quad f(X, Y) = g_D(a_1 X + b_1 Y, a_2 X + b_2 Y).$$

Hence we have

$$(4.2) \quad \begin{aligned} a &= g_D(a_1, a_2), \\ b &= \begin{cases} 2a_1 b_1 + 2D_1 a_2 b_2, & \text{if } D \equiv 0 \pmod{4}, \\ 2a_1 b_1 + a_1 b_2 + a_2 b_1 + 2D_1 a_2 b_2, & \text{if } D \equiv 3 \pmod{4}, \end{cases} \\ c &= g_D(b_1, b_2), \end{aligned}$$

and so  $q^{2s+1} | g_D(a_1, a_2)$  and  $q^{2s+1} | g_D(b_1, b_2)$ . Thus by lemma 1 we have  $q^{s+1} | a_1, q^{s+1} | a_2, q^{s+1} | b_1, q^{s+1} | b_2$ , and so from (4.2) we deduce that  $q^{2s+2} | a, q^{2s+2} | b, q^{2s+2} | c$ , that is,  $q^{2s+2} | d$ , which contradicts  $q^{2s+1} \parallel d$ . Thus we must have  $r_D(d) > 0$  if  $f(X, Y)$  is representable by  $g_D(X, Y)$ .

Conversely, we show that if  $r_D(d) > 0$ , then  $f(X, Y)$  is representable by  $g_D(X, Y)$ . We let

$$f'(X, Y) = d^{-1} f(X, Y) = a' X^2 + b' XY + c' Y^2,$$

so that  $a' = a/d, b' = b/d, c' = c/d$ . Thus by lemma 2  $f'(X, Y)$  is a primitive, positive-definite, binary quadratic form with

$$\text{discrim}(f'(X, Y)) = -Dk'^2,$$

where  $k'$  is a non-zero integer. Hence we have

$$b'^2 - 4a'c' = -Dk'^2, \quad \text{that is} \quad 4a'c' = b'^2 + Dk'^2.$$

If  $D \equiv 0 \pmod{4}$  then  $b'$  is even so that

$$(4.3)(a) \quad b' = 2b'', \quad a'c' = g_D(b'', k').$$

If  $D \equiv 3 \pmod{4}$  then  $b' - k'$  is even so that

$$(4.3)(b) \quad b' = 2b'' + k', \quad a'c' = g_D(b'', k').$$

Hence from (4.3)(a) and (4.3)(b) we have  $r_D(a'c') > 0$ . Now let  $q$  be a prime (possibly  $q=2$ ) dividing  $a'c'$ , which is such that  $(-D/q) = -1$ . Then by corollary 2 the highest power of  $q$  dividing  $a'c'$  is even, say  $q^{2\alpha} \parallel a'c'$ , and so from (4.3)(a)(b), by lemma 1, we have  $q^\alpha | b'', q^\alpha | k'$ . Now

$$\begin{aligned} 1 = \text{G.C.D.}(a', b', c') &= \text{G.C.D.}(a', 2b'', c'), & \text{if } D \equiv 0 \pmod{4}, \\ &= \text{G.C.D.}(a', 2b'' + k', c'), & \text{if } D \equiv 3 \pmod{4}, \end{aligned}$$

so that we have  $q^{2\alpha} \parallel a', q \nmid c'$  or  $q \nmid a', q^{2\alpha} \parallel c'$ . Treating every prime factor  $q$  of  $a'c'$ , which is such that  $(-D/q) = -1$ , in this way, we see that we may write

$$(4.4) \quad a' = P^2 A, \quad b'' = PQB, \quad c' = Q^2 C, \quad k' = PQK,$$

where  $P, Q$  are coprime integers all of whose prime factors  $q$  are such that  $(-D/q) = -1$ , and moreover  $A$  and  $C$  are free of such factors. From (4.3)(a)(b) and (4.4) we have

$$(4.5) \quad AC = g_D(B, K).$$

The only possible prime factors of  $A$  and  $C$  are the prime  $p(D)$  or primes  $p$  such that  $(-D/p) = +1$ . We let  $p_1, \dots, p_k$  denote the primes  $\neq p(D)$  which divide both  $A$  and  $C$ ;  $p_{k+1}, \dots, p_l$  the primes  $\neq p(D)$  which divide  $A$  but not  $C$ ;  $p_{l+1}, \dots, p_m$  the primes  $\neq p(D)$  which divide  $C$  but not  $A$ . Thus we have

$$(4.6) \quad (-D/p_i) = +1, \quad i = 1, \dots, m.$$

Hence we can set

$$(4.7) \quad A = p(D)^{\alpha_0} p_1^{\alpha_1} \dots p_k^{\alpha_k} p_{k+1}^{\alpha_{k+1}} \dots p_l^{\alpha_l},$$

and

$$(4.8) \quad C = p(D)^{\beta_0} p_1^{\beta_1} \dots p_k^{\beta_k} p_{l+1}^{\beta_{l+1}} \dots p_m^{\beta_m},$$

where  $0 \leq k \leq l \leq m$  and

$$\alpha_0 \geq 0, \quad \beta_0 \geq 0, \quad \alpha_i > 0, \quad i = 1, \dots, l; \quad \beta_j > 0, \quad j = 1, \dots, k, l+1, \dots, m.$$

Now let  $Q$  denote the rational number field and let  $Q((-D)^\dagger)$  (resp.  $Q((-D_1)^\dagger)$ ) denote the quadratic extension of  $Q$  formed by adjoining  $(-D)^\dagger$  (resp.  $(-D_1)^\dagger$ ). We let

$$\begin{aligned} \Delta_D &= Q((-D_1)^\dagger), & \text{if } D \equiv 0 \pmod{4}, \\ &= Q((-D)^\dagger), & \text{if } D \equiv 3 \pmod{4}, \end{aligned}$$

so that  $\text{discrim}(\Delta_D) = -D$ . The domain of all integers of  $\Delta_D$  is denoted by  $I(\Delta_D)$ . Factorization of elements of  $I(\Delta_D)$  into prime (equivalently irreducible) elements of  $I(\Delta_D)$  is unique for  $D = 3, 4, 7, 8, 11, 19, 43, 67, 163$  [5]. From (4.6) and corollary 2 we see that  $r_D(p_i) > 0$ ,  $i = 1, \dots, m$ . Thus there exist integers  $u_i$  and  $v_i$  such that

$$p_i = g_D(u_i, v_i), \quad i = 1, \dots, m.$$

Hence we have

$$p_i = \pi_i \bar{\pi}_i, \quad i = 1, \dots, m,$$

where

$$\begin{aligned} \pi_i &= u_i + v_i(-D_1)^\dagger, & \text{if } D \equiv 0 \pmod{4}, \\ &= u_i + \frac{1}{2}v_i + \frac{1}{2}v_i(-D)^\dagger, & \text{if } D \equiv 3 \pmod{4}, \end{aligned}$$

is an element of  $I(\Delta_D)$ . Moreover  $\pi_i$  and  $\bar{\pi}_i$  are conjugate, non-associated primes of  $I(\Delta_D)$ . Also by corollary 2 there exist integers  $u_0$  and  $v_0$  such that  $p(D) = g_D(u_0, v_0)$ ; in fact we can take



$$\begin{aligned} (u_0, v_0) &= (1, 1), & \text{if } D=4, \\ &= (0, 1), & \text{if } D=8, \\ &= (-1, +2), & \text{if } D=3, 7, 11, 19, 43, 67, 163. \end{aligned}$$

We set

$$\begin{aligned} \pi(D) &= u_0 + v_0(-D_1)^{\frac{1}{2}}, & \text{if } D \equiv 0 \pmod{4}, \\ &= u_0 + \frac{1}{2}v_0 + \frac{1}{2}v_0(-D)^{\frac{1}{2}}, & \text{if } D \equiv 3 \pmod{4}, \end{aligned}$$

so that

$$\begin{aligned} \pi(D) &= 1 + (-1)^{\frac{1}{2}}, & \text{if } D=4, \\ &= (-2)^{\frac{1}{2}}, & \text{if } D=8, \\ &= (-D)^{\frac{1}{2}}, & \text{if } D=3, 7, 11, 19, 43, 67, 163. \end{aligned}$$

As  $\pi(D)\overline{\pi(D)}=p(D)$ ,  $\pi(D)$  is a prime in  $I(\Delta_D)$ . Moreover its conjugate  $\overline{\pi(D)}$  is the associate  $\varepsilon(D)\pi(D)$  of  $\pi(D)$ , where  $\varepsilon(D)$  is the unit  $-(-1)^{\frac{1}{2}}$ , if  $D=4$ , and  $-1$ , otherwise. Hence the factorizations of  $A$  and  $C$  into primes in  $I(\Delta_D)$  are given by

$$A = \varepsilon(D)^{\alpha_0} \pi(D)^{2\alpha_0} \pi_1^{\alpha_1} \overline{\pi_1}^{\alpha_1} \dots \pi_k^{\alpha_k} \overline{\pi_k}^{\alpha_k} \pi_{k+1}^{\alpha_{k+1}} \overline{\pi_{k+1}}^{\alpha_{k+1}} \dots \pi_l^{\alpha_l} \overline{\pi_l}^{\alpha_l},$$

and

$$C = \varepsilon(D)^{\beta_0} \pi(D)^{2\beta_0} \pi_1^{\beta_1} \overline{\pi_1}^{\beta_1} \dots \pi_k^{\beta_k} \overline{\pi_k}^{\beta_k} \pi_{l+1}^{\beta_{l+1}} \overline{\pi_{l+1}}^{\beta_{l+1}} \dots \pi_m^{\beta_m} \overline{\pi_m}^{\beta_m}.$$

Thus from (4.5) we have

$$(4.9) \quad g_D(B, K) = \varepsilon(D)^{\alpha_0+\beta_0} \pi(D)^{2\alpha_0+2\beta_0} \pi_1^{\alpha_1+\beta_1} \overline{\pi_1}^{\alpha_1+\beta_1} \dots \pi_k^{\alpha_k+\beta_k} \overline{\pi_k}^{\alpha_k+\beta_k} \pi_{k+1}^{\alpha_{k+1}+\beta_{k+1}} \overline{\pi_{k+1}}^{\alpha_{k+1}+\beta_{k+1}} \dots \pi_l^{\alpha_l+\beta_l} \overline{\pi_l}^{\alpha_l+\beta_l} \pi_{l+1}^{\beta_{l+1}} \overline{\pi_{l+1}}^{\beta_{l+1}} \dots \pi_m^{\beta_m} \overline{\pi_m}^{\beta_m}.$$

Now let

$$(4.10) \quad \begin{aligned} h_D(B, K) &= B + K(-D_1)^{\frac{1}{2}}, & \text{if } D \equiv 0 \pmod{4}, \\ &= B + \frac{1}{2}K + \frac{1}{2}K(-D)^{\frac{1}{2}}, & \text{if } D \equiv 3 \pmod{4}, \end{aligned}$$

so that  $h_D(B, K)$  is an element of  $I(\Delta_D)$  such that

$$(4.11) \quad h_D(B, K) \overline{h_D(B, K)} = g_D(B, K).$$

Hence from (4.9) and (4.11) we have

$$(4.12) \quad \begin{aligned} h_D(B, K) &= \eta \pi(D)^{\alpha_0+\beta_0} \pi_1^{\gamma_1} \overline{\pi_1}^{\alpha_1+\beta_1-\gamma_1} \dots \pi_k^{\gamma_k} \overline{\pi_k}^{\alpha_k+\beta_k-\gamma_k} \\ &\quad \pi_{k+1}^{\gamma_{k+1}} \overline{\pi_{k+1}}^{\alpha_{k+1}+\beta_{k+1}-\gamma_{k+1}} \dots \pi_l^{\gamma_l} \overline{\pi_l}^{\alpha_l+\beta_l-\gamma_l} \pi_{l+1}^{\gamma_{l+1}} \overline{\pi_{l+1}}^{\beta_{l+1}-\gamma_{l+1}} \dots \pi_m^{\gamma_m} \overline{\pi_m}^{\beta_m-\gamma_m}, \end{aligned}$$

where  $\eta$  is a unit of  $I(\Delta_D)$  and  $\gamma_1, \dots, \gamma_m$  are integers such that

$$0 \leq \gamma_i \leq \begin{cases} \alpha_i + \beta_i, & i = 1, \dots, k, \\ \alpha_i, & i = k + 1, \dots, l, \\ \beta_i, & i = l + 1, \dots, m. \end{cases}$$

Now let  $s_i = \min(\alpha_i, \gamma_i)$ ,  $i = 1, \dots, k$ , so that  $s_i, \alpha_i - s_i, \gamma_i - s_i, \beta_i + s_i - \gamma_i$  are all non-negative integers, and set

$$\theta_1 = \eta \pi(D)^{\alpha_0} \pi_1^{\alpha_1} \bar{\pi}_1^{\alpha_1 - s_1} \dots \pi_k^{\alpha_k} \bar{\pi}_k^{\alpha_k - s_k} \pi_{k+1}^{\gamma_{k+1}} \bar{\pi}_{k+1}^{\alpha_{k+1} - \gamma_{k+1}} \dots \pi_l^{\gamma_l} \bar{\pi}_l^{\alpha_l - \gamma_l}$$

and

$$\theta_2 = \pi(D)^{\beta_0} \pi_1^{\gamma_1 - s_1} \bar{\pi}_1^{\beta_1 + s_1 - \gamma_1} \dots \pi_k^{\gamma_k - s_k} \bar{\pi}_k^{\beta_k + s_k - \gamma_k} \pi_{l+1}^{\gamma_{l+1}} \bar{\pi}_{l+1}^{\beta_{l+1} - \gamma_{l+1}} \dots \pi_m^{\gamma_m} \bar{\pi}_m^{\beta_m - \gamma_m}.$$

The numbers  $\theta_1$  and  $\theta_2$  are elements of  $I(\Delta_D)$  such that

$$(4.13) \quad \theta_1 \theta_2 = h_D(B, K), \quad \theta_1 \bar{\theta}_1 = A, \quad \theta_2 \bar{\theta}_2 = C.$$

Now as  $\theta_1, \theta_2$  are elements of  $I(\Delta_D)$  there exist rational integers  $R_1, R_2, S_1, S_2$  such that for  $i=1, 2$ ,

$$(4.14) \quad \theta_1 = R_1 + S_1(-D_1)^\dagger, \quad \theta_2 = R_2 + S_2(-D_1)^\dagger, \\ \text{if } D \equiv 0 \pmod{4}, \\ \theta_1 = R_1 + \frac{1}{2}S_1 + \frac{1}{2}S_1(-D)^\dagger, \quad \theta_2 = R_2 - \frac{1}{2}S_2 + \frac{1}{2}S_2(-D)^\dagger, \\ \text{if } D \equiv 3 \pmod{4}.$$

Hence from (4.10), (4.13) and (4.14) we have

$$(4.15) \quad B = R_1 R_2 - D_1 S_1 S_2, \quad K = R_1 S_2 + R_2 S_1, \\ \text{if } D \equiv 0 \pmod{4}, \\ B = R_1 R_2 - R_1 S_2 - D_1 S_1 S_2, \quad K = R_1 S_2 + R_2 S_1, \\ \text{if } D \equiv 3 \pmod{4}.$$

From (4.13) and (4.14) we obtain

$$(4.16) \quad A = g_D(R_1, S_1), \quad C = g_D(R_2, -S_2).$$

Now let

$$(4.17) \quad a_1' = PR_1, \quad a_2' = PS_1, \quad b_1' = QR_2, \quad b_2' = -QS_2.$$

Then from (4.3)(a)(b), (4.4), (4.15), (4.16) and (4.17) we obtain

$$(4.18) \quad a' = g_D(a_1', a_2'), \\ b' = \begin{cases} 2a_1' b_1' + 2D_1 a_2' b_2', & \text{if } D \equiv 0 \pmod{4}, \\ 2a_1' b_1' + a_1' b_2' + a_2' b_1' + 2D_1 a_2' b_2', & \text{if } D \equiv 3 \pmod{4}, \end{cases} \\ c' = g_D(b_1', b_2').$$

Thus from (4.18) we deduce that

$$f'(X, Y) = a' X^2 + b' XY + c' Y^2 = g_D(a_1' X + b_1' Y, a_2' X + b_2' Y).$$

Now as  $r_D(d) > 0$ , there exist integers  $u$  and  $v$  such that  $d = g_D(u, v)$ , so that

$$f(X, Y) = df'(X, Y) = g_D(u, v) g_D(a_1' X + b_1' Y, a_2' X + b_2' Y) \\ = g_D(a_1 X + b_1 Y, a_2 X + b_2 Y),$$

where

$$a_1 = ua_1' - D_1 va_2', \quad a_2 = ua_2' + va_1', \\ b_1 = ub_1' - D_1 vb_2', \quad b_2 = ub_2' + vb_1',$$

if  $D \equiv 0 \pmod{4}$ , and

$$\begin{aligned} a_1 &= ua_1' - D_1 va_2', & a_2 &= ua_2' + va_1' + va_2', \\ b_1 &= ub_1' - D_1 vb_2', & b_2 &= ub_2' + vb_1' + vb_2', \end{aligned}$$

if  $D \equiv 3 \pmod{4}$ . We note that

$$\begin{aligned} a_1 b_2 - a_2 b_1 &= (a_1' b_2' - a_2' b_1') g_D(u, v) \\ &= (a_1' b_2' - a_2' b_1') d \\ &= -PQ(R_1 S_2 + R_2 S_1) d = -PQKd = -k'd \neq 0. \end{aligned}$$

This completes the proof of theorem 1.

### 5. Number of representations.

This section is devoted to proving theorem 2. It suffices to count the number of representations of  $f(X, Y)$  by  $g_D(X, Y)$ . If  $f(X, Y)$  is not representable by  $g_D(X, Y)$  then by theorem 1  $r_D(d) = 0$  and so the number of representations  $= 0 = 2r_D(d)$ , as required. Hence we may suppose that  $f(X, Y)$  is representable by  $g_D(X, Y)$  (so that  $r_D(d) > 0$ ). Thus there exist integers  $a_1, a_2, b_1, b_2$  (with  $a_1 b_2 - a_2 b_1 \neq 0$ ) such that

$$(5.1) \quad f(X, Y) = g_D(a_1 X + b_1 Y, a_2 X + b_2 Y).$$

Now let

$$\begin{aligned} \alpha &= a_1 + a_2(-D_1)^{\frac{1}{2}}, & \text{if } D \equiv 0 \pmod{4}, \\ &= a_1 + \frac{1}{2}a_2 + \frac{1}{2}a_2(-D)^{\frac{1}{2}}, & \text{if } D \equiv 3 \pmod{4}, \end{aligned}$$

and

$$\begin{aligned} \beta &= b_1 + b_2(-D_1)^{\frac{1}{2}}, & \text{if } D \equiv 0 \pmod{4}, \\ &= b_1 + \frac{1}{2}b_2 + \frac{1}{2}b_2(-D)^{\frac{1}{2}}, & \text{if } D \equiv 3 \pmod{4}, \end{aligned}$$

so that  $\alpha$  and  $\beta$  are elements of  $I(\Delta_D)$  such that

$$(5.2) \quad f(X, Y) = (\alpha X + \beta Y)(\bar{\alpha} X + \bar{\beta} Y).$$

Hence the number of representations of  $f(X, Y)$  by  $g_D(X, Y)$  is just the number of ordered pairs  $(\alpha, \beta)$  of elements of  $I(\Delta_D)$  satisfying (5.2). Let  $(\alpha, \beta) = (\alpha_0, \beta_0)$  be a particular solution of (5.2) — we know at least one such solution exists. Since  $I(\Delta_D)$  is a unique factorization domain we can let  $\gamma_0 = \text{G.C.D.}(\alpha_0, \beta_0)$  and write  $\alpha_0 = \gamma_0 \alpha_0', \beta_0 = \gamma_0 \beta_0'$ , so that  $\text{G.C.D.}(\alpha_0', \beta_0') = 1$ . Hence we have

$$\text{G.C.D.}(\alpha_0' \bar{\alpha}_0', \alpha_0' \bar{\beta}_0' + \bar{\alpha}_0' \beta_0', \beta_0' \bar{\beta}_0') = 1,$$

and so

$$d = \text{G.C.D.}(a, b, c) = \text{G.C.D.}(\alpha_0 \bar{\alpha}_0, \alpha_0 \bar{\beta}_0 + \bar{\alpha}_0 \beta_0, \beta_0 \bar{\beta}_0) = \gamma_0 \bar{\gamma}_0.$$

Thus

$$d(\alpha_0' X + \beta_0' Y)(\bar{\alpha}_0' X + \bar{\beta}_0' Y) = (\alpha X + \beta Y)(\bar{\alpha} X + \bar{\beta} Y)$$

and so as  $\alpha_0'X + \beta_0'Y$  is a primitive, irreducible element of the unique factorization domain  $I(\Delta_D)[X, Y]$  we have

$$\alpha_0'X + \beta_0'Y \mid \alpha X + \beta Y \quad \text{or} \quad \alpha_0'X + \beta_0'Y \mid \bar{\alpha}X + \bar{\beta}Y .$$

If  $\alpha_0'X + \beta_0'Y \mid \alpha X + \beta Y$  there exists  $\delta \in I(\Delta_D)$  such that

$$\alpha X + \beta Y = \delta(\alpha_0'X + \beta_0'Y) ,$$

that is,

$$(\alpha, \beta) = (\delta\alpha_0', \delta\beta_0') , \quad \text{where } \delta\bar{\delta} = d .$$

Similarly if  $\alpha_0'X + \beta_0'Y \mid \bar{\alpha}X + \bar{\beta}Y$  we deduce that there exists  $\varepsilon \in I(\Delta_D)$  such that

$$(\alpha, \beta) = (\varepsilon\bar{\alpha}_0', \varepsilon\bar{\beta}_0') , \quad \text{where } \varepsilon\bar{\varepsilon} = d .$$

Thus there are  $2r_D(d)$  choices for  $(\alpha, \beta)$ , as required, unless

$$(\delta\alpha_0', \delta\beta_0') = (\varepsilon\bar{\alpha}_0', \varepsilon\bar{\beta}_0') ,$$

for some  $\delta, \varepsilon$  in  $I(\Delta_d)$  with  $\delta\bar{\delta} = \varepsilon\bar{\varepsilon} = d$ .

However, this is impossible, for otherwise

$$\begin{aligned} -Dk^2 &= b^2 - 4ac = (\alpha_0\bar{\beta}_0 + \bar{\alpha}_0\beta_0)^2 - 4(\alpha_0\bar{\alpha}_0)(\beta_0\bar{\beta}_0) \\ &= (\alpha_0\bar{\beta}_0 - \bar{\alpha}_0\beta_0)^2 \\ &= (\alpha_0'\bar{\beta}_0' - \bar{\alpha}_0'\beta_0')^2 d^2 = (\alpha_0'\beta_0' - \alpha_0'\beta_0')^2 \delta^2 \bar{\varepsilon}^2 = 0 , \end{aligned}$$

contradicting  $D \geq 3$ ,  $k \neq 0$ . This completes the proof of theorem 2.

## 6. Example.

We conclude this paper with a numerical example which illustrates theorems 1 and 2. We let

$$f_1(X, Y) = X^2 + 3XY + 4Y^2 \quad \text{and} \quad f_2(X, Y) = 4X^2 + 4XY + 8Y^2 .$$

Thus  $f_1(X, Y)$  and  $f_2(X, Y)$  are integral, positive-definite binary quadratic forms of discriminants  $-7$  and  $-7 \cdot 4^2$  respectively. The greatest common divisor of the coefficients of  $f_2(X, Y)$  is 4. By Dirichlet's theorem  $r_7(4) = 6$  so, by theorem 1,  $f_2(X, Y)$  is representable by  $f_1(X, Y)$ . Moreover by theorem 2 there are 12 such representations. Now  $g_7(X, Y) = X^2 + XY + 2Y^2$ , and we have

$$\begin{aligned} f_1(X, Y) &= g_7(X + Y, Y), \quad f_2(X, Y) = g_7(2X, 2Y) , \\ f_2(X, Y) &= f_1(2X - 2Y, 2Y) . \end{aligned}$$

We seek all 4-tuples of integers  $(a_1, a_2, b_1, b_2)$  with  $a_1b_2 - a_2b_1 \neq 0$  such that

$$f_2(X, Y) = f_1(a_1X + b_1Y, a_2X + b_2Y) ,$$

that is, such that,

$$f_1(a_1X + b_1Y, a_2X + b_2Y) = f_1(2X - 2Y, 2Y),$$

or

$$g_7((a_1 + a_2)X + (b_1 + b_2)Y, a_2X + b_2Y) = g_7(2X, 2Y).$$

Let

$$(6.1) \quad \alpha = a_1 + \frac{3}{2}a_2 + \frac{1}{2}a_2(-7)^{\frac{1}{2}}, \quad \beta = b_1 + \frac{3}{2}b_2 + \frac{1}{2}b_2(-7)^{\frac{1}{2}},$$

so that we want all ordered pairs  $(\alpha, \beta)$  of elements of  $I(Q((-7)^{\frac{1}{2}}))$  such that

$$\begin{aligned} (\alpha X + \beta Y)(\bar{\alpha}X + \bar{\beta}Y) &= (2X + (1 + (-7)^{\frac{1}{2}})Y)(2X + (1 - (-7)^{\frac{1}{2}})Y) \\ &= 4(X + \frac{1}{2}(1 + (-7)^{\frac{1}{2}})Y)(X + \frac{1}{2}(1 - (-7)^{\frac{1}{2}})Y). \end{aligned}$$

Since  $I(Q((-7)^{\frac{1}{2}}))[X, Y]$  is a unique factorization domain we have

$$X + \frac{1}{2}(1 + (-7)^{\frac{1}{2}})Y \mid \alpha X + \beta Y \quad \text{or} \quad X + \frac{1}{2}(1 + (-7)^{\frac{1}{2}})Y \mid \bar{\alpha}X + \bar{\beta}Y.$$

Thus we have  $\beta = \frac{1}{2}(1 \pm (-7)^{\frac{1}{2}})\alpha$ , where  $\alpha \bar{\alpha} = 4$ . All six solutions of this latter equation are given by

$$\alpha = \pm 2, \quad \frac{1}{2}(\pm 3 \pm (-7)^{\frac{1}{2}}).$$

Hence from (6.1) we have

$$\begin{aligned} (a_1, a_2, b_1, b_2) &= (2, 0, -2, 2), (-2, 0, 2, -2), (2, 0, 4, -2), (-2, 0, -4, 2), \\ &(0, 1, -4, 2), (0, -1, 4, -2), (0, 1, 4, -1), (0, -1, -4, 1), \\ &(3, -1, 1, 1), (-3, 1, -1, -1), (3, -1, 2, -2), (-3, 1, -2, 2) \end{aligned}$$

and so

$$\begin{aligned} f_2(X, Y) &= f_1(2X - 2Y, 2Y) &&= f_1(-2X + 2Y, -2Y), \\ &= f_1(2X + 4Y, -2Y) &&= f_1(-2X - 4Y, 2Y), \\ &= f_1(-4Y, X + 2Y) &&= f_1(4Y, -X - 2Y), \\ &= f_1(4Y, X - Y) &&= f_1(-4Y, -X + Y), \\ &= f_1(3X + Y, -X + Y) &&= f_1(-3X - Y, X - Y), \\ &= f_1(3X + 2Y, -X - 2Y) &&= f_1(-3X - 2Y, X + 2Y), \end{aligned}$$

REFERENCES

1. L. E. Dickson, *Introduction to the theory of numbers*, Dover Publications Inc., New York (1957), 78-79.
2. L. J. Mordell, *On the representation of a binary quadratic form as a sum of squares of linear forms*, Math. Z. 35 (1932), 1-15.
3. I. Niven, *Integers of quadratic fields as sums of squares*, Trans. Amer. Math. Soc. 48 (1940), 405-417.

4. G. Pall, *Sums of two squares in a quadratic field*, Duke Math. J. 18 (1951), 399–409.
5. H. M. Stark, *A complete determination of the complex quadratic fields of class-number one*, Michigan Math. J. 14 (1967), 1–27.

CARLETON UNIVERSITY, OTTAWA, CANADA