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 \( 3 \) \((\text{mod} \, 4)\) and we let

\[
D_1 = \frac{1}{4}D, \quad \text{if} \quad D \equiv 0 \,(\text{mod} \, 4),
\]

\[
= \frac{1}{4}(D + 1), \quad \text{if} \quad D \equiv 3 \,(\text{mod} \, 4).
\]

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 \( a_1 b_2 - a_2 b_1 \neq 0 \) such that

\[ f(X, Y) = g(a_1 X + b_1 \, Y, \, a_2 X + b_2 \, Y). \]

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

\[
\text{discrim}(f(X, Y)) = \text{discrim}(g(a_1 X + b_1 \, Y, \, a_2 X + b_2 \, Y))
\]

\[
= (a_1 b_2 - a_2 b_1)^2 \, \text{discrim}(g(X, Y)) = -Dk^2,
\]

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

Received February 13, 1971.
(1.1) \[ D = 3, 4, 7, 8, 11, 19, 43, 67, 163. \]

In this case the single reduced form is the principal form so that we have
\[
g(X, Y) = g_D(X, Y) = X^2 + D_1 Y^2, \quad \text{if } D \equiv 0 \pmod{4},
\]
\[
= X^2 + XY + D_1 Y^2, \quad \text{if } D \equiv 3 \pmod{4}.
\]

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, \( d = \gcd(a, b, c) \).

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 \( -D \), Pull [4] has proved the following theorem for the case \( D = 4 \).

**Theorem (Pull).** 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

\[
p(D) = \begin{cases} 2, & \text{if } D = 4, 8, \\ D, & \text{if } D = 3, 7, 11, 19, 43, 67, 163. \end{cases}
\]

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

\[
w_D = \begin{cases} 2, & \text{if } D = 7, 8, 11, 19, 43, 67, 163, \\ = 4, & \text{if } D = 4, \\ = 6, & \text{if } D = 3. \end{cases}
\]

and set

\[
h = p(D)^a 2^a p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s},
\]

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

\[
r_D(h) = \begin{cases} w_D \prod_{i=0}^{r} (\alpha_i + 1) \prod_{j=1}^{s} (1 + (-1)^{\beta_j}), & \text{if } D = 4, 7, 8 \text{ or } 8, \\ w_D \frac{1}{2} (1 + (-1)^a) \prod_{i=1}^{r} (\alpha_i + 1) \prod_{j=1}^{s} \frac{1}{2} (1 + (-1)^{\beta_j}), & \text{if } D = 3, 11, 19, 43, 67, 163. \end{cases}
\]

**Proof.** We begin by showing that for any positive integer \( k \) we have

\[
r_D(p(D)k) = r_D(k).
\]

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 \( \lambda : S_4(2k) \to S_4(k) \) defined by

\[
\lambda((x, y)) = \left(\frac{1}{2}(x+y), \frac{1}{2}(x-y)\right)
\]
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 \(\lambda : S_4(2k) \rightarrow S_4(k)\) defined by
\[
\lambda((x, y)) = (y, \frac{1}{2}x)
\]
is a bijection, so that \(|S_{D}(2k)| = |S_{D}(k)|\), that is, \(r_{D}(2k) = r_{D}(k)\). For \(D = 4\) 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
\[
h_1 = 2^{a_0} p_1^{\beta_1} \ldots p_r^{a_r} q_1^{\beta_1} \ldots q_s^{\beta_s} \quad \text{and} \quad \gcd(h_1, D) = 1,
\]
recalling that \(a_0 = 0\) 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
\[
r_{D}(h) = w_D \left\{ \sum_{e|e_0^i} (-D|e) \right\} \left\{ \prod_{i=1}^{n} \left( \sum_{e|e_i} (-D|e) \right) \right\} \left\{ \prod_{j=1}^{m} \left( \sum_{e|e'_j} (-D|e) \right) \right\}.
\]
Now as
\[
(-D/2) = +1, \quad \text{if} \ D = 7,
= 0, \quad \text{if} \ D = 4, 8,
= -1, \quad \text{if} \ D = 3, 11, 19, 43, 67, 163,
\]
we have
\[
\sum_{e|e_0^i} (-D|e) = \sum_{i=0}^{a_0} (-D/2)^i = \sum_{i=0}^{a_0} (-D/2)^i
\]
\[
= \begin{cases} 
\alpha_0 + 1, & \text{if} \ D = 4, 7, 8, \\
\frac{1}{2}(1 + (-1)^{\alpha_0}), & \text{if} \ D = 3, 11, 19, 43, 67, 163.
\end{cases}
\]
Also for \(i = 1, \ldots, r\) we have
\[
\sum_{e|p_i^i} (-D|e) = \sum_{i=0}^{\alpha_i} (-D|p_i)^i = \sum_{i=0}^{\alpha_i} (-D|p_i)^i = \alpha_i + 1,
\]
and for \(j = 1, \ldots, s\) we have
\[
\sum_{e|q_j^j} (-D|e) = \sum_{i=0}^{\beta_j} (-D|q_j)^i = \sum_{i=0}^{\beta_j} (-D|q_j)^i = \frac{1}{2}(1 + (-1)^{\beta_j}).
\]
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).** \( q = 2 \), \( D = 4 \) or 8.

As \( q = 2 \) we have \( (-D/q) = (-D/4) = 1 \). Now \( q^k | x^2 + D_1 y^2 \) and so as \( k \geq 1 \) we have \( q | x^2 + D_1 y^2 \). If \( q | y \) there exists an integer \( z \) such that \( yz = 1 \) (mod \( q \)) and so \( (x^2 + D_1 y^2) = -1 \) (mod \( q \)), which contradicts \( (-D/q) = -1 \). Hence we have \( q | x \), and so \( q | x \), say \( x = qx_1 \), \( y = qy_1 \). Moreover we have \( q^k | q^k(x_1^2 + D_1 y_1^2) \) and so if \( k \geq 2 \), \( q^{k-2} | x_1^2 + D_1 y_1^2 \).

If \( k \geq 3 \) we can continue in this way obtaining successively

\[
\begin{align*}
  x_1 &= qx_2, \\
  x_2 &= qx_3, \\
  \vdots \\
  x_{k-1} &= qx_k, \\
  x_k &= qx_{k+1},
\end{align*}
\]

\[
\begin{align*}
  y_1 &= qy_2, \\
  y_2 &= qy_3, \\
  \vdots \\
  y_{k-1} &= qy_k, \\
  y_k &= qy_{k+1},
\end{align*}
\]

If \( k \) is even the procedure terminates at this step and we have

\[
\begin{align*}
  x &= q^{k_1}x_{k+1}, \\
  y &= q^{k_1}y_{k+1},
\end{align*}
\]

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

\[
\begin{align*}
  x_{k+1} &= q^{k_1+1}x_{k+2}, \\
  y_{k+1} &= q^{k_1+1}y_{k+2},
\end{align*}
\]

that is,

\[
\begin{align*}
  x &= q^{k_1+1}x_{k+1}, \\
  y &= q^{k_1+1}y_{k+1},
\end{align*}
\]

or \( q^{k_1} | x \), \( q^{k_1} | y \).

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

Now \( q^k | x^2 + xy + D_1 y^2 \) and so we have \( q^k | (2x + y)^2 + D_1 y^2 \). If \( q \nmid y \) there exists an integer \( z \) such that \( yz = 1 \) (mod \( q \)) and so \((2x + y)z)^2 = -D \) (mod \( q \)),

\[
\begin{align*}
  \mathcal{F} \text{orms representable by an integral positive-definite \ldots} & \quad 77
\end{align*}
\]
which contradicts \((-D/q) = -1\). Hence \(q \mid y\) and so we have \(q \mid x\), say \(x = qx_1, y = qy_1\). Moreover if \(k \geq 2\) we have \(g^{k-2} | x_1^2 + x_1 y_1 + D_1 y_1^2\). 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 \(g_D(x, y) = x^2 + xy + D_1 y^2\), where \(D_1 = \frac{1}{4}(D+1)\) is an odd integer. Now \(2^k | x^2 + xy + D_1 y^2\) so that we have \(2 | x^2 + x + 1\), which is impossible as \(2 \mid x^2 + x\). Hence \(2 \mid y\) and so \(x = 2x_1\), \(y = 2y_1\). Moreover if \(k \geq 2\) we have \(2^{k-2} | x_1^2 + x_1 y_1 + D_1 y_1^2\), 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 \(d \mid k\). If \(D = 3, 7, 11, 19, 43, 67, 163\), this is clear, as in this case \(D\) is prime, and so \(d^2 \mid Dk^2\) implies \(d \mid k\). This leaves the cases \(D = 4\) and \(D = 8\). We let \(d = 2^a d_1\), where \(a \geq 0\) and \(d_1\) is odd. From \(b^2 - 4ac = -Dk^2\) we deduce that \(b\) must be even, say \(b = 2e\). Thus we have \(ac = e^2 + D_1 k^2\). Now \(2^a \mid d\) so that \(2^{2a} | ac = e^2 + D_1 k^2\), which implies that \(2^a \mid e\) and \(2^a \mid k\), since \(D_1 = 1\) or 2. Thus the discriminant of \(f'(X, Y)\) is the integer \(-Dk^2_1/d_1^2\), where \(k = 2^a k_1\). But \(d_1\) is odd so that as \(D = 4\) or 8 we must have \(d_1 \mid k_1\), say \(k_1 = d_1 k'\). 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 $q^{2s+1} | d$. 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

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

Hence we have

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

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 $q^{2s+1} | d$. Thus we must have $\rho_D(d) > 0$ if $f(X, Y)$ is representable by $g_D(X, Y)$.

Conversely, we show that if $\rho_D(d) > 0$, 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

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

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

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

Hence from (4.3)(a) and (4.3)(b) we have $\rho_D(a' c') > 0$. 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 $q^{2s} | a' c'$, and so from (4.3)(a)(b), by lemma 1, we have $q^{s} | b'', q^{s} | k'$. Now

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

so that we have $q^{2s} | a', q^{s} | c'$ or $q^{s} | a', q^{2s} | c'$. 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) \[ a' = P^2 A, \quad b'' = PQ B, \quad c' = Q^2 C, \quad k' = PQ K, \]
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
\[ \Delta C = g_{p_0}(B, K). \]
The only possible prime factors of \( A \) and \( C \) are the prime \( p(D) \) or primes \( p \) such that \((-D/p) = +1\). We let \( p_1, \ldots, p_k \) denote the primes \( \pm p(D) \) which divide both \( A \) and \( C \); \( p_{k+1}, \ldots, p_l \) the primes \( \pm p(D) \) which divide \( A \) but not \( C \); \( p_{l+1}, \ldots, p_m \) the primes \( \pm p(D) \) which divide \( C \) but not \( A \). Thus we have
\[ (-D/p_i) = +1, \quad i = 1, \ldots, m. \]
Hence we can set
\[ A = p(D)^{\alpha_0} p_1^{\alpha_1} \cdots p_k^{\alpha_k} p_{k+1}^{\beta_{k+1}} \cdots p_l^{\beta_l}, \]
and
\[ C = p(D)^{\alpha_0} p_1^{\beta_1} \cdots p_k^{\beta_k} p_{l+1}^{\beta_{l+1}} \cdots p_m^{\beta_m}, \]
where \( 0 \leq k \leq l \leq m \) and
\[ \alpha_0 \geq 0, \quad \beta_0 \geq 0, \quad \alpha_i > 0, \quad i = 1, \ldots, l; \quad \beta_j > 0, \quad j = 1, \ldots, k, l + 1, \ldots, m. \]
Now let \( Q \) denote the rational number field and let \( Q((-D)^i) \) (resp. \( Q((-D)^i) \)) denote the quadratic extension of \( Q \) formed by adjoining \((-D)^i\) (resp. \((-D)^i\)). We let
\[ \Delta_D = Q((-D)^i), \quad \text{if} \quad D \equiv 0 \pmod{4}, \]
\[ = Q((-D)^i), \quad \text{if} \quad D \equiv 3 \pmod{4}, \]
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 \( r_D(p_i) > 0, \ i = 1, \ldots, m. \)
Thus there exist integers \( u_i \) and \( v_i \) such that
\[ p_i = g_D(u_i, v_i), \quad i = 1, \ldots, m. \]
Hence we have
\[ p_i = \pi_i \bar{x}_i, \quad i = 1, \ldots, m, \]
where
\[ \pi_i = u_i + v_i (-D)^i, \quad \text{if} \quad D \equiv 0 \pmod{4}, \]
\[ = u_i + \frac{1}{2} v_i + \frac{1}{2} v_i (-D)^i, \quad \text{if} \quad D \equiv 3 \pmod{4}, \]
is an element of \( I(\Delta_D) \). Moreover \( \pi_i \) and \( \bar{x}_i \) 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
$$(u_0, v_0) = (1, 1), \quad \text{if } D = 4,$$
$$= (0, 1), \quad \text{if } D = 8,$$
$$= (-1, +2), \quad \text{if } D = 3, 7, 11, 19, 43, 67, 163.$$

We set
\[
\pi(D) = u_0 + v_0(-D)^{\frac{1}{4}}, \quad \text{if } D \equiv 0 \pmod{4},
\]
\[
= u_0 + \frac{1}{2}v_0 + \frac{1}{2}v_0(-D)^{\frac{1}{4}}, \quad \text{if } D \equiv 3 \pmod{4},
\]
so that
\[
\pi(D) = 1 + (-1)^{\frac{1}{4}}, \quad \text{if } D = 4,
\]
\[
= (-2)^{\frac{1}{4}}, \quad \text{if } D = 8,
\]
\[
= (-D)^{\frac{1}{4}}, \quad \text{if } D = 3, 7, 11, 19, 43, 67, 163.
\]

As $\pi(D)\bar{\pi}(D) = p(D)$, $\pi(D)$ is a prime in $I(\Delta_D)$. Moreover its conjugate $\bar{\pi}(D)$ is the associate $\varepsilon(D)\pi(D)$ of $\pi(D)$, where $\varepsilon(D)$ is the unit $-(-1)^{\frac{1}{4}}$, if $D = 4$, and $-1$, otherwise. Hence the factorizations of $A$ and $C$ into primes in $I(\Delta_D)$ are given by
\[
A = \varepsilon(D)^{a_1} \pi(D)^{2a_1 + 2a_2 + 2a_3 + \ldots + 2a_n + a_{n+1} + a_{n+2} + a_{n+3} + \ldots + a_k} \pi_1^{\alpha_1} \pi_2^{\alpha_2} \ldots \pi_k^{\alpha_k},
\]
and
\[
C = \varepsilon(D)^{b_1} \pi(D)^{2b_1 + 2b_2 + 2b_3 + \ldots + 2b_m + b_{m+1} + b_{m+2} + b_{m+3} + \ldots + b_l} \pi_1^{\beta_1} \pi_2^{\beta_2} \ldots \pi_m^{\beta_m}.
\]

Thus from (4.5) we have
\[
g_D(B, K) = \varepsilon(D)^{a_1 + b_1} \pi(D)^{2a_1 + 2b_1 + a_2 + b_2 + a_3 + b_3 + \ldots + a_k + b_k + a_{n+1} + b_{n+1} + a_{n+2} + b_{n+2} + a_{n+3} + b_{n+3} + \ldots + a_k} \pi_1^{\alpha_1} \pi_2^{\alpha_2} \ldots \pi_k^{\alpha_k},
\]
\[
= \varepsilon(D)^{a_1 + b_1} \pi(D)^{2a_1 + 2b_1 + a_2 + b_2 + a_3 + b_3 + \ldots + a_k + b_k + a_{n+1} + b_{n+1} + a_{n+2} + b_{n+2} + a_{n+3} + b_{n+3} + \ldots + a_k} \pi_1^{\alpha_1} \pi_2^{\alpha_2} \ldots \pi_k^{\alpha_k}.
\]

Now let
\[
h_D(B, K) = B + K(-D)^{\frac{1}{4}}, \quad \text{if } D \equiv 0 \pmod{4},
\]
\[
= B + \frac{1}{2}K + \frac{1}{2}K(-D)^{\frac{1}{4}}, \quad \text{if } D \equiv 3 \pmod{4},
\]
so that $h_D(B, K)$ is an element of $I(\Delta_D)$ such that
\[
h_D(B, K)h_D(B, K) = g_D(B, K).
\]

Hence from (4.9) and (4.11) we have
\[
h_D(B, K) = \eta \pi(D)^{a_1 + b_1} \pi_1^{\alpha_1} \pi_2^{\alpha_2} \ldots \pi_k^{\alpha_k} \pi_{n+1}^{\alpha_{n+1}} \pi_{n+2}^{\alpha_{n+2}} \ldots \pi_l^{\alpha_l} \pi_{m+1}^{\alpha_{m+1}} \pi_{m+2}^{\alpha_{m+2}} \ldots \pi_{l+m}^{\alpha_l} \pi_{l+m}^{\alpha_{l+m}},
\]
where $\eta$ is a unit of $I(\Delta_D)$ and $\gamma_1, \ldots, \gamma_m$ are integers such that
\[
0 \leq \gamma_i \leq \begin{cases} 
\alpha_i + \beta_i, & i = 1, \ldots, k, \\
\alpha_i, & i = k + 1, \ldots, l, \\
\beta_i, & i = l + 1, \ldots, m.
\end{cases}
\]

Now let $s_i = \min(\alpha_i, \gamma_i)$, $i = 1, \ldots, k$, 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

Math. Scand. — 6
\[ \theta_1 = \eta \pi(D)^{\sigma_0} \pi_1^{\sigma_1 - \sigma_2} \ldots \pi_k^{\sigma_k - \sigma_{k+1}} \pi_{k+1}^{\sigma_{k+1} - \sigma_{k+2}} \ldots \pi_m^{\sigma_m - \sigma} \]

and

\[ \theta_2 = \pi(D)^{\sigma_0} \pi_1^{\sigma_1 - \sigma_2} \ldots \pi_k^{\sigma_k - \sigma_{k+1} - \sigma_{k+2}} \ldots \pi_m^{\sigma_m - \sigma} \]

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

\[ \theta_1, \theta_2 = h_D(B, K), \quad \theta_1 \beta_1 = A, \quad \theta_2 \beta_2 = C. \]

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

\[ \theta_1 = R_1 + S_1(-D)^{\delta}, \quad \theta_2 = R_2 + S_2(-D)^{\delta}, \]

if \( D \equiv 0 \pmod{4} \),

\[ \theta_1 = R_1 + \frac{1}{2}S_1 + \frac{1}{2}S_1(-D)^{\delta}, \quad \theta_2 = R_2 - \frac{1}{2}S_2 + \frac{1}{2}S_2(-D)^{\delta}, \]

if \( D \equiv 3 \pmod{4} \).

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

\[ B = R_1 R_2 - D_1 S_1 S_2, \quad K = R_1 S_2 + R_2 S_1, \]

\[ B = R_1 R_2 - R_1 S_2 - D_1 S_1 S_2, \quad K = R_1 S_2 + R_2 S_1, \]

if \( D \equiv 0 \pmod{4} \),

\[ B = R_1 R_2 - R_1 S_2 - D_1 S_1 S_2, \quad K = R_1 S_2 + R_2 S_1, \]

if \( D \equiv 3 \pmod{4} \).

From (4.13) and (4.14) we obtain

\[ A = g_D(R_1, S_1), \quad C = g_D(R_2, -S_2). \]

Now let

\[ a'_1 = PR_1, \quad a'_2 = PS_1, \quad b'_1 = QR_2, \quad b'_2 = -QS_2. \]

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

\[ a' = g_D(a'_1, a'_2), \]

\[ b' = \begin{cases} 2a'_1b'_1 + 2D_1a'_2b'_2, & \text{if } D \equiv 0 \pmod{4}, \\ 2a'_1b'_1 + a'_2b'_2 + a'_2b'_1 + 2D_1a'_2b'_2, & \text{if } D \equiv 3 \pmod{4}, \end{cases} \]

\[ c' = g_D(b'_1, b'_2). \]

Thus from (4.18) we deduce that

\[ f'(X, Y) = a'X^2 + b'XY + c'Y^2 = g_D(a'_1X + b'_1Y, a'_2X + b'_2Y). \]

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

\[ f(X, Y) = df'(X, Y) = g_D(u, v)g_D(a'_1X + b'_1Y, a'_2X + b'_2Y) = g_D(a_1X + b_1Y, a_2X + b_2Y), \]

where

\[ a_1 = ua'_1 - D_1va'_2, \quad a_2 = ua'_2 + va'_1, \]

\[ b_1 = ub'_1 - D_1vb'_2, \quad b_2 = ub'_2 + vb'_1. \]
if \( D \equiv 0 \pmod{4} \), and
\[
\begin{align*}
    a_1 &= ua_1' - D_1 va_2', & a_2 &= ua_2' + va_1' + va_2', \\
    b_1 &= ub_1' - D_1 vb_2', & b_2 &= ub_2' + vb_1' + vb_2'.
\end{align*}
\]
if \( D \equiv 3 \pmod{4} \). We note that
\[
\begin{align*}
    a_1 b_2 - a_2 b_1 &= (a_1 b_2' - a_2 b_1') g_D(u,v) \\
    &= (a_1 b_2' - a_2 b_1') d \\
    &= -PQ(R_1 S_2 + R_2 S_1) d = -P Q K d = -k' d \neq 0.
\end{align*}
\]
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 is \( 0 = 2r_D(d) \), 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
\[
\begin{align*}
    \alpha &= a_1 + a_2 (-D_1)^{1/2}, \quad \text{if} \quad D \equiv 0 \pmod{4}, \\
    &= a_1 + a_2 (-D)^{1/4}, \quad \text{if} \quad D \equiv 3 \pmod{4},
\end{align*}
\]
and
\[
\begin{align*}
    \beta &= b_1 + b_2 (-D_1)^{1/2}, \quad \text{if} \quad D \equiv 0 \pmod{4}, \\
    &= b_1 + b_2 (-D)^{1/4}, \quad \text{if} \quad D \equiv 3 \pmod{4},
\end{align*}
\]
so that \( \alpha \) and \( \beta \) are elements of \( I(A_D) \) 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 \( I(A_D) \) 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 \( I(A_D) \) is a unique factorization domain we can let \( \gamma_0 = G.C.D.(\alpha_0, \beta_0) \) and write \( \alpha_0 = \gamma_0 \tilde{\alpha}_0', \beta_0 = \gamma_0 \tilde{\beta}_0' \), so that \( G.C.D.(\alpha_0', \beta_0') = 1 \). Hence we have
\[
G.C.D.(\alpha_0', \tilde{\alpha}_0', \alpha_0' \tilde{\beta}_0' + \tilde{\alpha}_0' \beta_0', \beta_0' \tilde{\beta}_0') = 1,
\]
and so
\[
\begin{align*}
    d &= G.C.D.(\alpha, \beta) = G.C.D.(\alpha_0 \tilde{\alpha}_0, \alpha_0 \tilde{\beta}_0 + \tilde{\alpha}_0 \beta_0, \beta_0 \tilde{\beta}_0) = \gamma_0 \tilde{\gamma}_0.
\end{align*}
\]
Thus
\[
\begin{align*}
    d(\alpha_0' X + \beta_0' Y)(\bar{\alpha}_0' X + \bar{\beta}_0' Y) = (\alpha X + \beta Y)(\bar{\alpha} X + \bar{\beta} Y)
\end{align*}
\]
and so as \(\alpha^\prime_0 X + \beta^\prime_0 Y\) is a primitive, irreducible element of the unique factorization domain \(I(\Delta_D)[X, Y]\) we have

\[
\alpha^\prime_0 X + \beta^\prime_0 Y \mid \alpha X + \beta Y \quad \text{or} \quad \alpha^\prime_0 X + \beta^\prime_0 Y \mid \bar{a}X + \bar{b}Y.
\]

If \(\alpha^\prime_0 X + \beta^\prime_0 Y \mid \alpha X + \beta Y\) there exists \(\delta \in I(\Delta_D)\) such that

\[
\alpha X + \beta Y = \delta(\alpha^\prime_0 X + \beta^\prime_0 Y),
\]

that is,

\[
(\alpha, \beta) = (\delta \alpha^\prime_0, \delta \beta^\prime_0), \quad \text{where} \quad \delta \delta = d.
\]

Similarly if \(\alpha^\prime_0 X + \beta^\prime_0 Y \mid \bar{a}X + \bar{b}Y\) we deduce that there exists \(\varepsilon \in I(\Delta_D)\) such that

\[
(\alpha, \beta) = (\varepsilon \bar{a}^\prime_0, \varepsilon \bar{b}^\prime_0), \quad \text{where} \quad \varepsilon \varepsilon = d.
\]

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

\[
(\delta \alpha^\prime_0, \delta \beta^\prime_0) = (\varepsilon \bar{a}^\prime_0, \varepsilon \bar{b}^\prime_0),
\]

for some \(\delta, \varepsilon \in I(\Delta_D)\) with \(\delta \delta = \varepsilon \varepsilon = d\).

However, this is impossible, for otherwise

\[
-Dk^2 = b^2 - 4ac = (\alpha_0 \bar{b}^\prime_0 + \bar{a} \beta_0)^2 - 4(\alpha_0 \bar{b}^\prime_0)(\beta_0 \bar{a}^\prime_0)
= (\alpha_0 \beta_0 - \bar{a} \beta_0)^2
= (\alpha^\prime_0 \beta^\prime_0 - \bar{a}^\prime_0 \beta^\prime_0)^2d^2 = (\alpha^\prime_0 \beta^\prime_0 - \alpha^\prime_0 \beta^\prime_0)^2 \beta^2 \varepsilon^2 = 0,
\]

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 \(r_3(4) = 6\) 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 \(g_2(X, Y) = X^2 + XY + 2Y^2\), and we have

\[
f_1(X, Y) = g_4(X + Y, Y), \quad f_2(X, Y) = g_4(2X, 2Y),
\]

\[
f_2(X, Y) = f_1(2X - 2Y, 2Y).
\]

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

\[
f_2(X, Y) = f_4(a_1X + b_1Y, a_2X + b_2Y),
\]
that is, such that,
\[ f_1(a_1X + b_1Y, a_2X + b_2Y) = f_1(2X - 2Y, 2Y), \]
or
\[ g_4(a_1 + a_2)X + (b_1 + b_2)Y, a_2X + b_2Y) = g_4(2X, 2Y). \]
Let
\[ \alpha = a_1 + \frac{1}{6}a_2 + \frac{1}{6}a_2(-7)^4, \quad \beta = b_1 + \frac{1}{6}b_2 + \frac{1}{6}b_2(-7)^4, \]
so that we want all ordered pairs \((\alpha, \beta)\) of elements of \(I(Q((-7)^4))\) such that
\[ (\alpha X + \beta Y)(\bar{\alpha}X + \bar{\beta}Y) = \left(2X + (1 + (-7)^4)Y\right)\left(2X + (1 - (-7)^4)Y\right) \]
\[ = 4\left(X + \frac{1}{2}(1 + (-7)^4)Y\right)\left(X + \frac{1}{2}(1 - (-7)^4)Y\right). \]
Since \(I(Q((-7)^4))[X, Y]\) is a unique factorization domain we have
\[ X + \frac{1}{2}(1 + (-7)^4)Y | \alpha X + \beta Y \quad \text{or} \quad X + \frac{1}{2}(1 + (-7)^4)Y | \bar{\alpha}X + \bar{\beta}Y. \]
Thus we have \(\beta = 4(1 \pm (-7)^4)x, \) where \(\alpha \bar{\alpha} = 4. \) All six solutions of this latter equation are given by
\[ \alpha = \pm 2, \quad \pm 3 \pm (-7)^4. \]
Hence from (6.1) we have
\[(a_1, a_2, b_1, b_2) = (2, 0, -2, 2), (-2, 0, 2, -2), (2, 0, 4, -2), (-2, 0, -4, 2), (0, 1, -4, 2), (0, 1, 4, -2), (0, -1, -4, 1), (0, -1, 4, 1), (3, -1, 1, 1), (-3, 1, -1, -1), (3, -1, 2, -2), (-3, 1, -2, 2)\]
and so
\[ f_2(X, Y) = f_1(2X - 2Y, 2Y) = f_1(-2X + 2Y, -2Y), \]
\[ = f_1(2X + 4Y, -2Y) = f_1(-2X - 4Y, 2Y), \]
\[ = f_1(-4Y, X + 2Y) = f_1(4Y, -X - 2Y), \]
\[ = f_1(4Y, X - Y) = f_1(-4Y, -X + Y), \]
\[ = f_1(3X + Y, -X + Y) = f_1(-3X - Y, X - Y), \]
\[ = f_1(3X + Y, -X - 2Y) = f_1(-3X - 2Y, X + 2Y), \]

REFERENCES


CARLETON UNIVERSITY, OTTAWA, CANADA