ACTA ARITHMETICA
LII (1989)

The class number of pairs of positive-definite binary quadratic forms

by

KENNETH HARDY(1) and KENNETH S. WILLIAMS(2) (Ottawa, Ont., Canada)

1. Introduction. Throughout this paper we write (a, b, c) for the binary quadratic form $ax^2+bxy+cy^2$. It will always be understood that the form (a, b, c) is *integral* (that is a, b, c are integers), *positive-definite* (equivalently $a > 0$, $b^2-4ac < 0$), and that its discriminant $d = b^2-4ac$ is a *fundamental* discriminant meaning that d has one of the following forms:

(1.1)(i) $$d = -p_1 p_2 \dots p_n \equiv 1 \pmod 4,$$

(1.1)(ii) $$d = -4p_2 \dots p_n \equiv 12 \pmod{16},$$

(1.1)(iii) $$d = -8p_2 \dots p_n \equiv 8 \pmod{16},$$

where $p_1, \dots, p_n$ denote distinct odd primes and n is the total number of distinct prime divisors of d. As d is fundamental, the form (a, b, c) is *primitive*, that is GCD $(a, b, c) = 1$.

We say that the pair of forms $((a, b, c), (A, B, C))$ is equivalent to the pair of forms $((a_1, b_1, c_1), (A_1, B_1, C_1))$, written

$$((a, b, c), (A, B, C)) \sim ((a_1, b_1, c_1), (A_1, B_1, C_1)),$$

if there exist integers p, q, r, s with $ps-qr = +1$ such that

$$a(px+qy)^2+b(px+qy)(rx+sy)+c(rx+sy)^2 = a_1 x^2+b_1 xy+c_1 y^2$$

and

$$A(px+qy)^2+B(px+qy)(rx+sy)+C(rx+sy)^2 = A_1x^2+B_1xy+C_1y^2.$$

The discriminants $d = b^2-4ac$ and $D = B^2-4AC$ as well as the codiscriminant $\Delta = bB-2aC-2cA$ remain invariant under $\sim$. It is easy to verify that

(1) Research supported by Natural Sciences and Engineering Research Council of Canada Grant A-8049.

(2) Research supported by Natural Sciences and Engineering Research Council of Canada Grant A-7233.

$\sim$ is an equivalence relation on the set of pairs of forms with prescribed values of d, D and Δ, and that the number $h(d, D, \Delta)$ of equivalence classes is finite [3]. The main result of this paper is an explicit formula for $h(d, D, \Delta)$. In Section 3 we prove the following theorem.

THEOREM. *Let d (<0) and D (<0) be the discriminants (equal to fundamental discriminants) and Δ (<0) the codiscriminant of a pair of integral, positive-definite binary quadratic forms. Assume that $\Delta^2 > dD$ and that* GCD $(dD, \Delta) = 2^a$, *for some integer $a \geqslant 0$. Set*

$$c(d, D, \Delta) = \begin{cases} 1, & \text{if } d \equiv 1 \pmod 4, \\ \Delta^*, & \text{if } d \equiv 8 \pmod{16}, \\ & \text{or } d \equiv 12 \pmod{16},\ D \equiv 8,12 \pmod{16}, \\ 3-\Delta^*, & \text{if } d \equiv 12 \pmod{16},\ D \equiv 1 \pmod 4, \end{cases} \tag{1.2}$$

where

$$\Delta^* = \begin{cases} 2, & \text{if } \Delta \equiv 0 \pmod 4, \\ 1, & \text{if } \Delta \equiv 2 \pmod 4. \end{cases} \tag{1.3}$$

Then we have

$$h(d, D, \Delta) = c(d, D, \Delta) \sum_{e \mid (\Delta^2 - dD)/4} \left(\frac{d}{e}\right) = c(D, d, \Delta) \sum_{e \mid (\Delta^2 - dD)/4} \left(\frac{D}{e}\right). \tag{1.4}$$

Before giving the proof of this theorem we make some remarks. We first note that if d and D are the discriminants and Δ the codiscriminant of a pair of positive-definite forms then $\Delta < 0$. This is clear as

$$\begin{aligned} \Delta &= bB - 2aC - 2cA \leqslant |bB| - 2aC - 2cA \\ &< \sqrt{(b^2-d)(B^2-D)} - 2(aC+cA) \quad (\text{as } d<0,\ D<0) \\ &= 4\sqrt{acAC} - 2(aC+cA) = -2(\sqrt{aC} - \sqrt{cA})^2 \leqslant 0. \end{aligned}$$

Next we note that $\Delta^2 \geqslant dD$ follows from the identity

$$a^2(\Delta^2 - dD) = \left((2ac-b^2)A + abB - 2a^2C\right)^2 - d(bA - aB)^2. \tag{1.5}$$

It is easy to show from (1.5) that the possibility $\Delta^2 = dD$, which is excluded from the theorem, occurs if and only if $a = A$, $b = B$, $c = C$. Thus, in this case, $h(d, D, \Delta)$ is just the number $h(d)$ of classes of forms of discriminant d. Dirichlet gave a formula for $h(d)$ in 1839. We also note that the identity

$$\Delta^2 - dD = 4\left((aC - cA)^2 - (aB - bA)(bC - cB)\right) \tag{1.6}$$

show that $(\Delta^2 - dD)/4$ is always an integer.

The condition GCD $(dD, \Delta) = 2^a$, for some integer $a \geqslant 0$, is imposed in the theorem for two reasons. The first reason is so that appeal can be made in the proof of the theorem to the following result of Dirichlet: Let d (<0) be a fundamental discriminant and let m be a positive integer such that GCD $(m, d) = 2^a$ for some integer $a \geqslant 0$. Then the number $\Psi_d(m)$ of representations of m by the forms of a representative system of positive-definite, integral, binary quadratic forms of discriminant d is given by

$$\Psi_d(m) = w(d) \sum_{e \mid m} \left(\frac{d}{e}\right), \tag{1.7}$$

where e runs through the positive divisors of m and

$$w(d) = \begin{cases} 2, & \text{if } d < -4, \\ 4, & \text{if } d = -4, \\ 6, & \text{if } d = -3. \end{cases} \tag{1.8}$$

The second reason for the inclusion of the condition GCD $(dD, \Delta) = 2^a$ $(a \geqslant 0)$ is so that we have

$$\text{GCD}\ (e_1, d) = \text{GCD}(e_1, D) = \text{GCD}(e_1, \Delta) = 1,$$

for any odd integer e_1 dividing $(\Delta^2 - dD)/4$, and thus

$$\left(\frac{dD}{e_1}\right) = \left(\frac{\Delta^2}{e_1}\right) = 1, \quad \left(\frac{d}{e_1}\right) = \left(\frac{D}{e_1}\right),$$

which enables us to relate the sums

$$\sum_{e \mid (\Delta^2 - dD)/4} \left(\frac{d}{e}\right) \quad \text{and} \quad \sum_{e \mid (\Delta^2 - dD)/4} \left(\frac{D}{e}\right)$$

in a simple manner (see (1.9) below). Without the condition GCD $(dD, \Delta) = 2^a$ $(a \geqslant 0)$ our theorem is no longer valid. For example take $d = -7$, $D = -7$, $\Delta = -21$ so that GCD $(dD, \Delta) =$ GCD $(49, 21) = 7$. In this case every pair of forms with $d = -7$, $D = -7$, $\Delta = -21$ is equivalent to one of the four inequivalent pairs

$$\begin{aligned} &((1, 1, 2), (2, -5, 4)), \\ &((1, 1, 2), (2, 9, 11)), \\ &((1, 1, 2), (4, -3, 1)), \\ &((1, 1, 2), (4, 11, 8)), \end{aligned}$$

so that $h(-7, -7, -21) = 4$. However we have

$$c(-7, -7, -21) = 1, \quad (\Delta^2 - dD)/4 = 98,$$

and

$$\begin{aligned} \sum_{e \mid 98} \left(\frac{-7}{e}\right) &= \left(\frac{-7}{1}\right) + \left(\frac{-7}{2}\right) + \left(\frac{-7}{7}\right) + \left(\frac{-7}{14}\right) + \left(\frac{-7}{49}\right) + \left(\frac{-7}{98}\right) \\ &= 1+1+0+0+0+0 = 2. \end{aligned}$$

Next we show that

$$\sum_{e\mid(\Delta^2-dD)/4}\left(\frac{d}{e}\right)=k(d,D,\Delta)\sum_{e\mid(\Delta^2-dD)/4}\left(\frac{D}{e}\right), \tag{1.9}$$

where

$$k(d,D,\Delta)=\begin{cases}\Delta^*, & \text{if } d\equiv 1\pmod 4,\ D\equiv 8\pmod{16},\\ 3-\Delta^*, & \text{if } d\equiv 1\pmod 4,\ D\equiv 12\pmod{16},\\ 1/\Delta^*, & \text{if } d\equiv 8\pmod{16},\ D\equiv 1\pmod 4,\\ 1/(3-\Delta^*), & \text{if } d\equiv 12\pmod{16},\ D\equiv 1\pmod 4,\\ 1, & \text{otherwise.}\end{cases} \tag{1.10}$$

Since

$$k(d,D,\Delta)=\frac{c(D,d,\Delta)}{c(d,D,\Delta)} \tag{1.11}$$

this establishes the right hand equality of (1.4). Thus to prove the theorem it suffices to prove just the left hand equality of (1.4).

We define the nonnegative integer m by

$$2^m\|(\Delta^2-dD)/4,$$

and, for $e\mid(\Delta^2-dD)/4$, we set

$$e=2^\varepsilon e_1,$$

where

$$0\leqslant\varepsilon\leqslant m,\quad e_1\geqslant 1,\quad e_1\equiv 1\pmod 2,\quad e_1\mid(\Delta^2-dD)/4.$$

As GCD $(dD,\Delta)=2^a$ $(a\geqslant 0)$, we have

$$\mathrm{GCD}(e_1,d)=\mathrm{GCD}(e_1,D)=\mathrm{GCD}(e_1,\Delta)=1,$$

and

$$\left(\frac{dD}{e_1}\right)=\left(\frac{\Delta^2}{e_1}\right)=1,\quad \left(\frac{d}{e_1}\right)=\left(\frac{D}{e_1}\right),$$

so that

$$\sum_{e_1\mid(\Delta^2-dD)/4}\left(\frac{d}{e_1}\right)=\sum_{e_1\mid(\Delta^2-dD)/4}\left(\frac{D}{e_1}\right).$$

Hence to complete the proof of (1.9) it suffices to prove

$$\sum_{\varepsilon=0}^{m}\left(\frac{d}{2}\right)^\varepsilon=k(d,D,\Delta)\sum_{\varepsilon=0}^{m}\left(\frac{D}{2}\right)^\varepsilon.$$

Table 1

d	D	Δ	(dD,Δ)	$E=(\Delta^2-dD)/4$	$c(d,D,\Delta)$	$\sum_{e\mid E}\left(\frac{d}{e}\right)$	$c(D,d,\Delta)$	$\sum_{e\mid E}\left(\frac{D}{e}\right)$	representative system of inequivalent pairs of forms	$h(d,D,\Delta)$
−3	−7	−5	1	1	1	1	1	1	((1, 1, 1), (1, 1, 2))	1
−3	−8	−10	2	19	1	2	1	2	((1, 1, 1), (1, 4, 6)) ((1, 1, 1), (6, 4, 1))	2
−7	−4	−8	4	9	1	1	1	1	((1, 1, 2), (2, 2, 1))	1
−7	−4	−6	2	2	1	2	2	1	((1, 1, 2), (1, 0, 1)) ((1, 1, 2), (1, 2, 2))	2
−8	−24	−16	16	16	2	1	2	1	((1, 0, 2), (1, 0, 6)) ((1, 0, 2), (3, 0, 2))	2
−8	−24	−22	2	73	1	2	1	2	((1, 0, 2), (3, 6, 5)) ((1, 0, 2), (3, −6, 5))	2
−8	−4	−8	8	8	2	1	2	1	((1, 0, 2), (1, 2, 2)) ((1, 0, 2), (1, −2, 2))	2
−8	−4	−10	2	17	1	2	1	2	((1, 0, 2), (2, 2, 1)) ((1, 0, 2), (2, −2, 1))	2
−4	−20	−12	4	16	2	1	2	1	((1, 0, 1), (1, 0, 5)) ((1, 0, 1), (3, 4, 3))	2
−4	−20	−42	2	421	1	2	1	2	((1, 0, 1), (3, 14, 18)) ((1, 0, 1), (3, −14, 18))	2

This is clear as

$$\left(\frac{d}{2}\right)=\left(\frac{D}{2}\right)=0, \text{ if } d\equiv 8 \text{ or } 12 \pmod{16},\ D\equiv 8 \text{ or } 12 \pmod{16},$$

$$\left(\frac{d}{2}\right)=\left(\frac{D}{2}\right), \text{ if } d\equiv D\equiv 1 \pmod 4,\ d\equiv D \pmod 8,$$

$$m=0, \text{ if } d\equiv D\equiv 1 \pmod 4,\ d\not\equiv D \pmod 8,$$

$$m=1, \left(\frac{d}{2}\right)=1, \text{ if } d\equiv 1 \pmod 4,\ D\equiv 8 \pmod{16},\ \Delta\equiv 0 \pmod 4,$$

$$m=0, \text{ if } d\equiv 1 \pmod 4,\ D\equiv 8 \pmod{16},\ \Delta\equiv 2 \pmod 4,$$

$$m=0, \text{ if } d\equiv 1 \pmod 4,\ D\equiv 12 \pmod{16},\ \Delta\equiv 0 \pmod 4,$$

$$m=1, \text{ if } d\equiv 1 \pmod 4,\ D\equiv 12 \pmod{16},\ D\equiv 2 \pmod 4.$$

We conclude this section by giving a short table of values illustrating the theorem (Table 1).

2. Preliminary lemmas and propositions. In this section, we recall and prove some results about the equivalence of forms which we will need in the proof of the theorem in Section 3. If the forms (a, b, c) and (a_1, b_1, c_1) are equivalent we write $(a, b, c) \sim (a_1, b_1, c_1)$. Two equivalent forms possess the same discriminant and $\sim$ is an equivalence relation on the set of forms with discriminant d. The equivalence class containing all forms equivalent to the form (a, b, c) is denoted by $[a, b, c]$. The number of equivalence classes is finite and is denoted by $h(d)$. Next we recall how classes of forms of the same discriminant d are multiplied together. The product of two classes $[a_1, b_1, c_1]$ and $[a_2, b_2, c_2]$ is defined as follows: forms $(a, b, a'c)$ and (a', b, ac) with GCD $(a, a') = 1$ are chosen so that

$$[a_1, b_1, c_1] = [a, b, a'c], \quad [a_2, b_2, c_2] = [a', b, ac],$$

and the product $[a_1, b_1, c_1]\,[a_2, b_2, c_2]$ is defined by

$$[a, b, a'c][a', b, ac] = [aa', b, c] \tag{2.1}$$

(see for example [1], Chapter XIII, § 1).

The set $H(d)$ of classes of forms of discriminant d under multiplication is a finite abelian group of order $h(d)$. The identity class I is given by

$$I = \begin{cases} [1, 0, -d/4], & \text{if } d\equiv 0 \pmod 4, \\ [1, 1, (1-d)/4], & \text{if } d\equiv 1 \pmod 4. \end{cases} \tag{2.2}$$

The inverse of the class $[a, b, c]$ is the class $[a, b, c]^{-1} = [a, -b, c] = [c, b, a]$. The subgroup of squares in $H(d)$ has traditionally been called the principal genus.

A class $[a, b, c]$ is called *ambiguous* if $[a, b, c]^2 = I$. Gauss showed that there are 2^{n-1} ambiguous classes. These can be written in the form $[A_i]$ $(i = 1, 2, \ldots, 2^{n-1})$, where each A_i is a form of the type

$$A_i = (a_i, b_i, c_i), \tag{2.3}$$

where

$$a_i > 0, \quad b_i^2 - 4a_i c_i = d, \tag{2.4}$$

and

$$b_i = 0 \quad \text{or} \quad a_i. \tag{2.5}$$

Gauss also showed that the principal genus consists of $h(d)/2^{n-1}$ classes, say $[F_j]$ $(j = 1, 2, \ldots, h(d)/2^{n-1})$. Replacing each F_j by an equivalent form, if necessary, we may suppose that

$$F_j = (f_j^2, g_j, h_j) \quad (j = 1, 2, \ldots, h(d)/2^{n-1}), \tag{2.6}$$

where

$$f_j > 0, \quad \mathrm{GCD}(f_j, 2d) = 1, \tag{2.7}$$

and

$$g_j^2 - 4f_j^2 h_j = d. \tag{2.8}$$

For $1 \leqslant i \leqslant 2^{n-1}$ and $1 \leqslant j \leqslant h(d)/2^{n-1}$ we see from (2.4) and (2.8) that

$$g_j^2 \equiv d \equiv b_i^2 \pmod 4,$$

so that $g_j \equiv b_i \pmod 2$, showing that $\frac{1}{2}(g_j - b_i)$ is an integer. Further we note that

$$\mathrm{GCD}(a_i, f_j) \mid a_i \mid d, \quad \mathrm{GCD}(a_i, f_j) \mid f_j,$$

so that, as $\mathrm{GCD}(f_j, d) = 1$, we must have

$$\mathrm{GCD}(a_i, f_j) = 1. \tag{2.9}$$

Hence, for $1 \leqslant i \leqslant 2^{n-1}$ and $1 \leqslant j \leqslant h(d)/2^{n-1}$, we can define u_{ij} to be the least non-negative solution of

$$a_i u_{ij} \equiv \tfrac{1}{2}(g_j - b_i) \pmod{f_j}. \tag{2.10}$$

We set

$$v_{ij} = (a_i u_{ij} - \tfrac{1}{2}(g_j - b_i))/f_j \tag{2.11}$$

and

$$k_{ij} = 2a_i u_{ij} + b_i = 2f_j v_{ij} + g_j. \tag{2.12}$$

Squaring (2.12), and appealing to (2.4) and (2.8), we obtain

$$a_i(a_i u_{ij}^2+b_i u_{ij}+c_i) = f_j(f_j v_{ij}^2+g_j v_{ij}+f_j h_j).$$

Since $\mathrm{GCD}(a_i, f_j) = 1$ we can define an integer l_{ij} by

$$l_{ij} = \frac{a_i u_{ij}^2+b_i u_{ij}+c_i}{f_j} = \frac{f_j v_{ij}^2+g_j v_{ij}+f_j h_j}{a_i}. \tag{2.13}$$

We now define the *join* $A_i \circ F_j$ of the forms A_i and F_j to be the form

$$A_i \circ F_j = (a_i f_j, k_{ij}, l_{ij}). \tag{2.14}$$

Since $a_i f_j > 0$ and

$$k_{ij}^2-4a_i f_j l_{ij} = d, \tag{2.15}$$

we see that $A_i \circ F_j$ is a positive-definite form of discriminant d.

LEMMA 1. *For $i = 1, 2, \ldots, 2^{n-1}$ and $j = 1, 2, \ldots, h(d)/2^{n-1}$ we have*

$$[A_i \circ F_j] = [a_i, b_i, c_i][f_j, g_j, f_j h_j].$$

Proof. We have

$$\begin{aligned}[a_i, b_i, c_i][f_j, g_j, f_j h_j] &= [a_i, 2a_i u_{ij}+b_i, a_i u_{ij}^2+b_i u_{ij}+c_i]\\ &\quad [f_j, 2f_j v_{ij}+g_i, f_j v_{ij}^2+g_j v_{ij}+f_j h_j]\\ &= [a_i, k_{ij}, f_j l_{ij}]\,[f_j, k_{ij}, a_i l_{ij}] = [a_i f_j, k_{ij}, l_{ij}] = [A_i \circ F_j].\end{aligned}$$

LEMMA 2. *For $i, r = 1, 2, \ldots, 2^{n-1}$ and $j, s = 1, 2, \ldots, h(d)/2^{n-1}$, we have*

$$[A_i \circ F_j] = [A_r \circ F_s] \Leftrightarrow (i, j) = (r, s).$$

Proof. It clearly suffices to prove that $[A_i \circ F_j] = [A_r \circ F_s] \Rightarrow (i, j) = (r, s)$. Suppose $[A_i \circ F_j] = [A_r \circ F_s]$. Then, by Lemma 1, we have

$$[a_i, b_i, c_i][f_j, g_j, f_j h_j] = [a_r, b_r, c_r][f_s, g_s, f_s h_s]. \tag{2.16}$$

Squaring (2.16), we obtain, as

$$[a_i, b_i, c_i]^2 = [a_r, b_r, c_r]^2 = I,$$

that

$$[f_j, g_j, f_j h_j]^2 = [f_s, g_s, f_s h_s]^2.$$

Hence we have

$$[f_j^2, g_j, h_j] = [f_s^2, g_s, h_s],$$

and so $j = s$. Then, from (2.16), we obtain $[a_i, b_i, c_i] = [a_r, b_r, c_r]$, so that $i = r$. This completes the proof of Lemma 2.

From Lemma 2 we have immediately the following proposition.

PROPOSITION 1. *The forms $A_i \circ F_j$ $(i = 1, 2, \ldots, 2^{n-1};\ j = 1, 2, \ldots, h(d)/2^{n-1}$ form a set of $h(d)$ inequivalent forms of discriminant d.*

LEMMA 3. *For $i = 1, 2, \ldots, 2^{n-1}$ and $j = 1, 2, \ldots, h(d)/2^{n-1}$*

$$m_{ij} = 2(v_{ij}^2-h_j)/a_i, \quad n_{ij} = k_{ij}/a_i, \tag{2.17}$$

are integers.

Proof. From (2.5) and (2.12) we have $k_{ij} = 2a_i u_{ij}+b_i \equiv 0 \pmod{a_i}$ so that n_{ij} is an integer. Then, by (2.12), we deduce that $2f_j v_{ij}+g_j \equiv 0 \pmod{a_i}$. Hence we have

$$g_j^2 \equiv 4f_j^2 v_{ij}^2 \begin{cases} \pmod{a_i}, & \text{if } a_i \text{ odd},\\ \pmod{2a_i}. & \text{if } a_i \text{ even}.\end{cases}$$

Also, from (2.4) and (2.8), we have

$$g_j^2 = 4f_j^2 h_j+b_i^2-4a_i c_i \equiv 4f_j^2 h_j \begin{cases} \pmod{a_i}, & \text{if } a_i \text{ odd},\\ \pmod{2a_i}, & \text{if } a_i \text{ even}.\end{cases}$$

Hence we have

$$4f_j^2(v_{ij}^2-h_j) \equiv \begin{cases} 0 \pmod{a_i}, & \text{if } a_i \text{ odd},\\ 0 \pmod{2a_i}, & \text{if } a_i \text{ even}.\end{cases}$$

Since $\mathrm{GCD}(a_i, f_j) = 1$ we deduce that

$$\begin{aligned} v_{ij}^2-h_j &\equiv 0 \pmod{a_i}, && \text{if } a_i \text{ odd},\\ 2(v_{ij}^2-h_j) &\equiv 0 \pmod{a_i}, && \text{if } a_i \text{ even}.\end{aligned}$$

This completes the proof that m_{ij} is an integer.

LEMMA 4. *For $i = 1, 2, \ldots, 2^{n-1}$ and $j = 1, 2, \ldots, h(d)/2^{n-1}$, we have*

$$f_j^2 m_{ij}^2+2g_j m_{ij} n_{ij}+4h_j n_{ij}^2 = 4l_{ij}^2, \tag{2.18}$$

$$2f_j^2 m_{ij} v_{ij}+f_j g_j m_{ij}+2g_j n_{ij} v_{ij}+4f_j h_j n_{ij} = 2k_{ij} l_{ij}, \tag{2.19}$$

$$4f_j(f_j v_{ij}^2+g_j v_{ij}+f_j h_j) = k_{ij}^2-d, \tag{2.20}$$

$$a_i(f_j^2 m_{ij}+g_j n_{ij}) = 2a_i f_j l_{ij}+d. \tag{2.21}$$

Proof. Equations (2.18) and (2.19) follow using (2.12), (2.13) and (2.17); equation (2.20) follows using (2.13) and (2.15); equation (2.21) follows using (2.8), (2.12), (2.13) and (2.17).

PROPOSITION 2. *For $i = 1, 2, \ldots, 2^{n-1}$ and $j = 1, 2, \ldots, h(d)/2^{n-1}$ the following is an identity in the variables A, B, C:*

$$\begin{aligned}(2l_{ij}A-k_{ij}B+2a_i f_j C)^2-d(B^2-4AC) &\equiv f_j^2(m_{ij}A-2v_{ij}B+2a_i C)^2\\ &\quad +g_j(m_{ij}A-2v_{ij}B+2a_i C)(2n_{ij}A-2f_j B)+h_j(2n_{ij}A-2f_j B)^2.\end{aligned} \tag{2.22}$$

Proof. The coefficients of A^2, AB, B^2, AC on both sides of (2.22) agree in view of (2.18), (2.19), (2.20), (2.21) respectively. The coefficients of C^2 are clearly both $4a_i^2 f_j^2$. Finally the coefficients of BC are the same by (2.12). This completes the proof of Proposition 2.

LEMMA 5. *For* $i = 1, 2, \ldots, 2^{n-1}$ *and* $j = 1, 2, \ldots, h(d)/2^{n-1}$ *we have*

$$g_i n_{ij} - \frac{d}{a_i} \equiv 0 \pmod{f_j} \tag{2.23}$$

and

$$g_j l_{ij} - \frac{d}{a_i} v_{ij} \equiv 0 \pmod{f_j}. \tag{2.24}$$

Proof. By (2.17), (2.12), (2.8), we have

$$\begin{aligned} g_j n_{ij} - d/a_i &= (g_i k_{ij} - d)/a_i \\ &= ((2f_j g_j v_{ij} + g_j^2) - (g_j^2 - 4f_j^2 h_j))/a_i \\ &= f_j(2g_j v_{ij} + 4f_j h_j)/a_i. \end{aligned}$$

Since $\mathrm{GCD}(a_i, f_j) = 1$ and $g_j n_{ij} - d/a_i$ is an integer, we see that $(2g_j v_{ij} + 4f_j h_j)/a_i$ is an integer, and so $g_j n_{ij} - d/a_i$ is a multiple of f_j. This completes the proof of (2.23). The proof of (2.24) is similar.

3. Proof of Theorem. Let (f, F) be a pair of forms with discriminants d and D and codiscriminant Δ. Then, by Proposition 1, we have

$$(f, F) \sim (A_i \circ F_j, G),$$

for a unique pair (i, j) of integers with $1 \leqslant i \leqslant 2^{n-1}$ and $1 \leqslant j \leqslant h(d)/2^{n-1}$, and a form $G = (A, B, C)$, satisfying

$$A > 0, \quad B^2 - 4AC = D, \tag{3.1}$$

and

$$k_{ij} B - 2l_{ij} A - 2a_i f_j C = \Delta. \tag{3.2}$$

Now $(A_i \circ F_j, G_1) \sim (A_i \circ F_j, G_2)$ if and only if an automorph of $A_i \circ F_j$ transforms G_1 into G_2. The form $A_i \circ F_j$ possesses exactly $w(d)$ automorphs [4: Theorem 202]. However only half of these automorphs give rise to different G's. Hence we have

$$h(d, D, \Delta) = \frac{1}{w(d)/2} \sum_{i=1}^{2^{n-1}} \sum_{j=1}^{h(d)/2^{n-1}} \sum_{(A,B,C)}{}' 1 \tag{3.3}$$

where the dash (′) indicates that A, B, C must satisfy (3.1) and (3.2).

Appealing to Proposition 2, we see that (3.1) and (3.2) are equivalent to

$$A > 0, \tag{3.4}$$

$$2l_{ij} A - k_{ij} B + 2a_i f_j C = -\Delta, \tag{3.5}$$

$$\begin{aligned} \Delta^2 - dD = f_j^2 (m_{ij} A - 2v_{ij} B + 2a_i C)^2 \\ + g_j (m_{ij} A - 2v_{ij} B + 2a_i C)(2n_{ij} A - 2f_j B) + h_j (2n_{ij} A - 2f_j B)^2. \end{aligned} \tag{3.6}$$

Changing the summation variables A, B, C in (3.3) to A, X, Y by means of

$$X = \left(m_{ij} - \frac{2v_{ij} n_{ij}}{f_j}\right) A + 2a_i C + \frac{2v_{ij}}{f_j} Y, \tag{3.7}$$

$$Y = n_{ij} A - f_j B, \tag{3.8}$$

we obtain

$$h(d, D, \Delta) = \frac{2}{w(d)} \sum_{i=1}^{2^{n-1}} \sum_{j=1}^{h(d)/2^{n-1}} \sum_{(A,X,Y)}{}' 1, \tag{3.9}$$

where the dash (′) now indicates that the sum is restricted to those (A, X, Y) satisfying

$$\Delta^2 - dD = f_j^2 X^2 + 2g_j XY + 4h_j Y^2, \tag{3.10}$$

$$A > 0, \tag{3.11}$$

$$-\frac{d}{a_i} A + f_j^2 X + g_j Y = -f_j \Delta, \tag{3.12}$$

$$X \equiv \left(m_{ij} - \frac{2v_{ij} n_{ij}}{f_j}\right) A + \frac{2v_{ij}}{f_j} Y \pmod{2a_i}, \tag{3.13}$$

$$Y \equiv n_{ij} A \pmod{f_j}. \tag{3.14}$$

Eliminating A from (3.11), (3.12), (3.13) and (3.14), we obtain

$$h(d, D, \Delta) = \frac{2}{w(d)} \sum_{i=1}^{2^{n-1}} \sum_{j=1}^{h(d)/2^{n-1}} \sum_{(X,Y)}{}' 1, \tag{3.15}$$

where the dash (′) indicates that the sum is restricted to those pairs of integers (X, Y) satisfying

$$\Delta^2 - dD = f_j^2 X^2 + 2g_j XY + 4h_j Y^2, \tag{3.16}$$

$$f_j^2 X + g_j Y + f_j \Delta < 0, \tag{3.17}$$

$$f_j^2 X + g_j Y + f_j \Delta \equiv 0 \pmod{d/a_i}, \tag{3.18}$$

$$f_j^2 n_{ij} X + \left(g_j n_{ij} - \frac{d}{a_i}\right) Y + f_j n_{ij} \Delta \equiv 0 \pmod{f_j d/a_i}, \tag{3.19}$$

$$f_j\left(2f_j l_{ij}+\frac{d}{a_i}\right)X+2\left(g_j l_{ij}-\frac{d}{a_i}v_{ij}\right)Y+2f_j l_{ij}\Delta \equiv 0 \pmod{2df_j}. \tag{3.20}$$

Next we observe that (3.17) is redundant as it follows from (3.16). We have

$$\begin{aligned}(f_j^2 X+g_j Y)^2 &= f_j^2(f_j^2 X^2+2g_j XY)+g_j^2 Y^2\\ &= f_j^2(\Delta^2-dD-4h_j Y^2)+g_j^2 Y^2\\ &= f_j^2(\Delta^2-dD)+dY^2\\ &< f_j^2\Delta^2 \quad (\text{as } d<0,\ D<0),\end{aligned}$$

so that (as $\Delta<0$) we have

$$f_j\Delta < f_j^2 X+g_j Y < -f_j\Delta,$$

which implies (3.17).

Next we show that (3.19) is also redundant. As $\mathrm{GCD}(d, f_j)=1$, we have $\mathrm{GCD}(d/a_i, f_j)=1$, so that (3.19) is equivalent to

$$(g_j n_{ij}-d/a_i)\,Y \equiv 0 \pmod{f_j}, \tag{3.21}$$

and

$$f_j^2 n_{ij} X+g_j n_{ij} Y+f_j n_{ij}\Delta \equiv 0 \pmod{d/a_i}. \tag{3.22}$$

Clearly, by Lemma 5, (3.21) imposes no condition on Y, and (3.22) follows trivially from (3.18).

Similarly, as $\mathrm{GCD}(2d, f_j)=1$, (3.20) is equivalent to

$$2\left(g_j l_{ij}-\frac{d}{a_i}v_{ij}\right)Y \equiv 0 \pmod{f_j} \tag{3.23}$$

and

$$f_j\left(2f_j l_{ij}+\frac{d}{a_i}\right)X+2\left(g_j l_{ij}-\frac{d}{a_i}v_{ij}\right)Y+2f_j l_{ij}\Delta \equiv 0 \pmod{2d}, \tag{3.24}$$

and (3.23) is redundant by Lemma 5. Further, as $\Delta^2-dD \equiv 0 \pmod 4$, from (3.16), we see that X must be even, and we can replace X by $2X$ in (3.17), (3.18), (3.24). Summarizing we have

$$h(d, D, \Delta)=\frac{2}{w(d)}\sum_{j=1}^{h(d)/2^{n-1}}\sum_{i=1}^{2^{n-1}}{\sum_{(X,Y)}}' 1, \tag{3.25}$$

where the dash (′) indicates that X and Y must satisfy

$$(\Delta^2-dD)/4 = f_j^2 X^2+g_j XY+h_j Y^2, \tag{3.26}$$

$$2f_j^2 X+g_j Y+f_i\Delta \equiv 0 \pmod{d/a_i}, \tag{3.27}$$

$$f_j\left(2f_j l_{ij}+\frac{d}{a_i}\right)X+\left(g_j l_{ij}-\frac{d}{a_i}v_{ij}\right)Y+f_j l_{ij}\Delta \equiv 0 \pmod d. \tag{3.28}$$

It is now convenient to consider the three cases (1.1) (i) (ii) (iii) separately. We just treat the case (1.1) (i), $d=-p_1 p_2 \dots p_n \equiv 1 \pmod 4$, as the other two cases can be handled similarly. In this case the forms $A_i (i=1, 2, \dots, 2^{n-1})$ are given exactly twice each by $(w, w, \frac{1}{4}(w-d/w))$, as w runs through the positive divisors of d. Let $u_i \equiv u_j(w)$ be the least nonnegative solution of

$$wu_j \equiv \tfrac{1}{2}(g_j-w) \pmod{f_j}, \tag{3.29}$$

and define $v_j \equiv v_j(w)$ by

$$v_j=(wu_j-\tfrac{1}{2}(g_j-w))/f_j. \tag{3.30}$$

Hence, in the notation of Section 2, we have

$$\begin{cases}a_i = w, & b_i = w, & c_i = \frac{1}{4}(w-d/w),\\ u_{ij}=u_j, & v_{ij}=v_j, & l_{ij}=(f_j v_j^2+g_j v_j+f_j h_j)/w.\end{cases} \tag{3.31}$$

Hence in this case we have

$$h(d, D, \Delta)=\frac{1}{w(d)}\sum_{j=1}^{h(d)/2^{n-1}}\sum_{w|d}{\sum_{(X,Y)}}' 1, \tag{3.32}$$

where the dash (′) indicates that X, Y must satisfy

$$(\Delta^2-dD)/4 = f_j^2 X^2+g_j XY+h_j Y^2, \tag{3.33}$$

$$2f_j^2 X+g_j Y \equiv -f_j\Delta \pmod{d/w}, \tag{3.34}$$

$$(f_j v_j^2+g_j v_j+f_j h_j)(2f_j^2 X+g_j Y+f_j\Delta)+d(f_j X-v_j Y) \equiv 0 \pmod{dw}. \tag{3.35}$$

Since $w \mid d$ and d is squarefree, we have $(w, d/w)=1$, and congruence (3.35) is equivalent to

$$(f_j v_j^2+g_j v_j+f_j h_j)(2f_j^2 X+g_j Y+f_j\Delta)+d(f_j X-v_j Y) \equiv 0 \pmod{w^2}, \tag{3.36}$$

in view of (3.34). Now, appealing to (2.8), we see that (3.36) is equivalent to

$$\begin{aligned}&(2f_j^3 v_j^2+2f_j^2 g_j v_j-2f_j^3 h_j+f_j g_j^2)\,X\\ &+(f_j g_j v_j^2+4f_j^2 h_j v_j+f_j g_j h_j)\,Y+(f_j^2 v_j^2+f_j g_j v_j+f_j^2 h_j)\Delta \equiv 0 \pmod{w^2}.\end{aligned} \tag{3.37}$$

Next, as $k_{ij} \equiv 0 \pmod w$, we have

$$2f_j v_j+g_j \equiv 0 \pmod w, \tag{3.38}$$

so

$$(g_j+2f_j v_j)^2 \equiv 0 \pmod{w^2}, \tag{3.39}$$

giving

$$g_j^2 \equiv -4f_j g_j v_j - 4f_j^2 v_j^2 \pmod{w^2}. \tag{3.40}$$

Also, as $g_j^2 - 4f_j^2 h_j = d \equiv 0 \pmod{w}$, we have

$$4f_j^2 h_j \equiv g_j^2 \equiv 4f_j^2 v_j^2 \pmod{w}. \tag{3.41}$$

As $(f_j, w) = 1$ and w is odd, (3.41) gives

$$h_j \equiv v_j^2 \pmod{w}. \tag{3.42}$$

Then, from (3.38) and (3.42), we have

$$(g_j + 2f_j v_j)(h_j - v_j^2) \equiv 0 \pmod{w^2},$$

and so

$$g_j h_j \equiv g_j v_j^2 - 2f_j h_j v_j + 2f_j v_j^3 \pmod{w^2}. \tag{3.43}$$

Using (3.40) and (3.43) in (3.37), we see that (3.37) is equivalent to

$$(f_j v_j^2 + g_j v_j + f_j h_j)(2f_j^2 X + g_j Y - f_j \Delta) \equiv 0 \pmod{w^2}. \tag{3.44}$$

We now show that $2f_i^2 X + g_i Y - f_j \Delta \equiv 0 \pmod{w}$. This is trivial if $w = 1$ so we can exclude this possibility. We have already noted that $f_j v_j^2 + g_j v_j + f_j h_j \equiv 0 \pmod{w}$. We show that $f_j v_j^2 + g_j v_j + f_j h_j \not\equiv 0 \pmod{w^2}$. Suppose that $f_j v_j^2 + g_j v_j + f_j h_j \equiv 0 \pmod{w^2}$. Then $l_{ij} \equiv 0 \pmod{w}$, and so, as $k_{ij} \equiv 0 \pmod{w}$, we have $d = k_{ij}^2 - 4w f_j l_{ij} \equiv 0 \pmod{w^2}$, which contradicts that d is squarefree. Thus (3.44) is equivalent to

$$2f_j^2 X + g_j Y \equiv f_j \Delta \pmod{w}. \tag{3.45}$$

Hence we have shown that

$$h(d, D, \Delta) = \frac{1}{w(d)} \sum_{j=1}^{h(d)/2^{n-1}} \sum_{w \mid d} \sum_{(X,Y)}{}' 1, \tag{3.46}$$

where the dash (′) indicates that X, Y must satisfy

$$(\Delta^2 - dD)/4 = f_j^2 X^2 + g_j XY + h_j Y^2, \tag{3.47}$$

$$2f_j^2 X + g_j Y \equiv -f_j \Delta \pmod{d/w}, \tag{3.48}$$

$$2f_j^2 X + g_j Y \equiv f_j \Delta \pmod{w}. \tag{3.49}$$

Any solution (X, Y) of (3.47) must satisfy

$$(2f_j^2 X + g_j Y)^2 \equiv f_j^2 \Delta^2 \pmod{d},$$

so that

$$2f_j^2 X + g_j Y \equiv \pm f_j \Delta \pmod{k},$$

for every divisor k of d. Thus we have

$$h(d, D, \Delta) = \frac{1}{w(d)} \sum_{j=1}^{h(d)/2^{n-1}} \sum_{(X,Y)}{}' 1. \tag{3.50}$$
$$(\Delta^2 - dD)/4 = f_j^2 X^2 + g_j XY + h_j Y^2$$

Since $(\Delta^2 - dD)/4$ can only be represented by forms of discriminant d whose classes lie in the principal genus, and $\mathrm{GCD}((\Delta^2 - dD)/4, d) = 1$, by Dirichlet's theorem [2: Theorem 64] [4: Theorem 204], we have

$$h(d, D, \Delta) = \sum_{e \mid (\Delta^2 - dD)/4} \left(\frac{d}{e}\right) \tag{3.51}$$

as asserted. This completes the proof.

4. Acknowledgement. One of the authors (K. S. Williams) would like to acknowledge financial support from Arizona State University, which enabled him to complete some of this paper at the university during February 1986.

References

[1] H. Cohn, *A Second Course in Number Theory*, John Wiley & Sons, Inc., New York, N. Y., 1962.

[2] L. E. Dickson, *Introduction to the Theory of Numbers*, University of Chicago Press, Chicago, Illinois, 1929.

[3] C. Hooley, *On the diophantine equation* $ax^2 + by^2 + cz^2 + 2fyz + 2gzx + 2hxy = 0$, Arch. Math. 19 (1968), 472–478.

[4] E. Landau, *Elementary Number Theory*, Chelsea Publishing Company, New York, N. Y., 1958.

DEPARTMENT OF MATHEMATICS AND STATISTICS
CARLETON UNIVERSITY
Ottawa, Ontario, Canada K1S 5B6

Received on 14.5.1987
and in revised form on 22.10.1987 (1722)