The genera representing a positive integer

by

PIERRE KAPLAN (Nancy) and KENNETH S. WILLIAMS (Ottawa)

1. Introduction. A nonsquare integer d with $d \equiv 0$ or 1 (mod 4) is called a *discriminant*. Let H(d) denote the group of strict equivalence classes of primitive, integral, binary quadratic forms $(a, b, c) = ax^2 + bxy + cy^2$ of discriminant $b^2 - 4ac = d$ under Gaussian composition. Only positive-definite forms are used if d < 0. H(d) is a finite abelian group called the *form class* group. The order |H(d)| of H(d) is called the *form class number* and is denoted by h(d). The class of the form (a, b, c) is denoted by [a, b, c]. The *conductor* of the discriminant d is the largest positive integer f such that d/f^2 is a discriminant. The *fundamental discriminant* associated with dis $\Delta = d/f^2$. Let G(d) denote the genus group of H(d), that is, G(d) = $H(d)/H^2(d)$. The order |G(d)| of G(d) is a power of 2 so that there exists a nonnegative integer t(d) such that

(1)
$$|G(d)| = 2^{t(d)}$$
.

The quantity $2^{t(d)}$ is the number of classes in H(d) whose order divides 2, that is, the number of ambiguous classes in H(d). The value of t(d) is given by [1, §153, pp. 409–413; §151, pp. 400–407], [2, p. 277]

(2)
$$t(d) = \begin{cases} \omega(d) & \text{if } d \equiv 0 \pmod{32}, \\ \omega(d) - 2 & \text{if } d \equiv 4 \pmod{16}, \\ \omega(d) - 1 & \text{otherwise,} \end{cases}$$

where $\omega(d)$ denotes the number of distinct prime factors of d. We do not use the explicit value of t(d) in any of the proofs in this paper but we do make use of it in the examples in Section 4.

Let n denote a positive integer. We say that n is represented by the form (a, b, c) if there exist integers x and y such that $n = ax^2 + bxy + cy^2$. The representation is said to be proper if (x, y) = 1. If n is represented by

²⁰⁰⁰ Mathematics Subject Classification: Primary 11E25.

Key words and phrases: binary quadratic forms, genera.

Research of the second author was supported by Natural Sciences and Engineering Research Council of Canada grant A-7233.

(a, b, c) then n is represented by (a_1, b_1, c_1) for any $(a_1, b_1, c_1) \in [a, b, c]$ so we say that n is represented by the class [a, b, c]. Further, we say that n is represented by the genus G of G(d) if n is represented by at least one class in G. We let

(3) $G(n,d) = \{G \in G(d) \mid n \text{ is represented by } G\}, \quad g(n,d) = |G(n,d)|,$

so that

(4) g(n, d) = number of genera of discriminant d representing n.

Gauss's original definition of genera was by means of generic characters (see for example [1, \S 121–122, pp. 313–319]), and was done in such a way that if n is prime to d and is represented by some class of discriminant d then n is represented by exactly one genus of discriminant d. A main result of genus theory (see [1, \S 158, pp. 432–433]) is that the genera defined as we did above and the genera defined through generic characters coincide, so that we have

LEMMA 1. If n is represented by a class of discriminant d and (n, d) = 1then g(n, d) = 1.

We have two aims in this paper. First we show that G(n, d) is always a coset of a subgroup of G(d) and then we give an explicit formula for g(n, d) without the restriction (n, d) = 1. Before stating our result, we give some more notation.

It is convenient to define the positive integers M, Q and U as follows:

(5) M = M(n, d) is the largest integer such that $M^2 | n, M | f$,

(6)
$$U = U(n,d) = \prod_{p|d, p \nmid f} p^{v_p(n)},$$

(7)
$$Q = Q(n,d) = U(n/M^2, d/M^2) = \prod_{p|d/M^2, p \nmid f/M} p^{v_p(n/M^2)},$$

where $p^{v_p(k)}$ denotes the largest power of the prime p dividing the nonzero integer k. A prime p is said to be a *null prime* with respect to n and d if

(8)
$$v_p(n) \equiv 1 \pmod{2}, \quad v_p(n) < 2v_p(f).$$

The set of all null primes with respect to n and d is denoted by Null(n, d). If Null $(n, d) \neq \emptyset$ it is shown in [2, Proposition 4.1] for d < 0 that n is not represented by any form of discriminant d. The proof is exactly the same for d > 0. It is also shown in [2, Lemma 4.1(a)] for d < 0 that if Null(n, d) $= \emptyset$ then

(9)
$$(n/M^2, f/M) = 1$$

and

(10)
$$(n/M^2Q, d/M^2) = 1.$$

Again the proof is independent of the sign of d.

Let *m* be a positive integer dividing *f* and let *K* be a class in H(d). The following assertions can be deduced from [1, §§150–151, pp. 397–407], [2, Lemma 6.1], and [3, Theorem 1] in the equivalent language of ideals.

- (i) K contains a form (a, b, c) with (a, m) = 1, $m \mid b$ and $m^2 \mid c$;
- (ii) the mapping $\theta_m : H(d) \to H(d/m^2)$ given by

$$\theta_m([a, b, c]) = [a, b/m, c/m^2]$$

is a surjective homomorphism.

As $\theta_m(H^2(d)) \subseteq H^2(d/m^2)$, the surjective homomorphism

$$\theta_m: H(d) \to H(d/m^2)$$

induces a surjective homomorphism

(11)
$$\theta_m: G(d) \to G(d/m^2)$$

by

(12)
$$\widetilde{\theta}_m(KH^2(d)) = \theta_m(K)H^2(d/m^2).$$

We prove

THEOREM. Suppose that the positive integer n is represented by the genus $G \in G(d)$. Then the set G(n,d) of genera of discriminant d which represent n is given by

$$G(n,d) = G \ker \theta_M$$

and the number g(n, d) of genera representing n by

$$g(n,d) = 2^{t(d)-t(d/M^2)},$$

where M is defined in (5), $\tilde{\theta}_M$ in (11) and (12), t(d) in (1) (see also (2)).

The Theorem is proved in Section 3 after some lemmas are proved in Section 2. Three examples illustrating the Theorem are given in Section 4.

2. Some lemmas. We begin by proving the following result which is central to everything that we do.

LEMMA 2. Let $G \in G(d)$. The positive integer n is represented by G if and only if n/M^2 is represented by $\tilde{\theta}_M(G)$.

Proof. Suppose that n is represented by the genus $G \in G(d)$. Then there exists a class $K \in G$ which represents n. By property (i) above, the class K contains a form (a, b, c) with

(13)
$$(a, M) = 1, \quad M \mid b, \quad M^2 \mid c.$$

As (a, b, c) represents n, there exist integers x and y such that

(14)
$$n = ax^2 + bxy + cy^2.$$

Completing the square in (14), we obtain

(15)
$$4an = (2ax + by)^2 - dy^2.$$

As $M^2 | n$ and $M^2 | d$ (by (5)), we see from (15) that M | 2ax + by. As M | b we have M | 2ax. As (a, M) = 1 we deduce that M | 2x. If M is odd we have M | x. If M is even we have $M_1 | x$, where $M_1 = M/2$. Then, from

$$4(n/M^2) = a(x/M_1)^2 + 2(b/M)(x/M_1)y + 4(c/M^2)y^2,$$

we deduce that $2 | a(x/M_1)^2$. As 2 | M and (a, M) = 1 we have (a, 2) = 1 so that $2 | x/M_1$. Thus M | x. Hence in both cases we have M | x and so

$$n/M^2 = a(x/M)^2 + (b/M)(x/M)y + (c/M^2)y^2,$$

showing that n/M^2 is represented by

$$[a, b/M, c/M^2] = \theta_M([a, b, c]) \in \widetilde{\theta}_M([a, b, c]H^2(d)) = \widetilde{\theta}_M(G).$$

Now suppose that n/M^2 is represented by the class L of the genus $\tilde{\theta}_M(G) \in G(d/M^2)$. Let $K_1 \in H(d)$ be such that $G = K_1 H^2(d)$, so that

$$LH^2(d/M^2) = \widetilde{\theta}_M(G) = \theta_M(K_1)H^2(d/M^2).$$

Thus there exists $L_1 \in H(d/M^2)$ such that $L = \theta_M(K_1)L_1^2$. As $\theta_M : H(d) \to H(d/M^2)$ is surjective there exists $K_2 \in H(d)$ such that $\theta_M(K_2) = L_1$ so that setting $K = K_1K_2^2$ we have $L = \theta_M(K)$. By property (i) we can choose K = [a, b, c] with (a, M) = 1, $M \mid b$, $M^2 \mid c$ so that

$$L = \theta_M(K) = \theta_M([a, b, c]) = [a, b/M, c/M^2].$$

As L represents n/M^2 there exist integers x and y such that $n/M^2 = ax^2 + (b/M)xy + (c/M^2)y^2$ so that $n = aX^2 + bXy + cy^2$ with X = xM. Thus n is represented by [a, b, c] = K and so by the genus G.

Lemma 3. $G(n,d)=\widetilde{\theta}_M^{-1}(G(n/M^2,d/M^2)).$

Proof. Let $G \in G(n, d)$. Then $G \in G(d)$ represents n. Hence, by Lemma 2, n/M^2 is represented by $\tilde{\theta}_M(G) \in G(d/M^2)$. Thus $\tilde{\theta}_M(G) \in G(n/M^2, d/M^2)$ so that $G \in \tilde{\theta}_M^{-1}(G(n/M^2, d/M^2))$. We have shown that

(16)
$$G(n,d) \subseteq \widetilde{\theta}_M^{-1}(G(n/M^2, d/M^2)).$$

Now suppose that $G \in \widetilde{\theta}_M^{-1}(G(n/M^2, d/M^2))$, so that $G \in G(d)$ and $\widetilde{\theta}_M(G) \in G(n/M^2, d/M^2)$. Hence $\widetilde{\theta}_M(G) \in G(d/M^2)$ represents n/M^2 . By Lemma 2 we deduce that n is represented by G. Hence $G \in G(n, d)$, proving that

(17)
$$\widetilde{\theta}_M^{-1}(G(n/M^2, d/M^2)) \subseteq G(n, d).$$

The required result follows from (16) and (17). \blacksquare

LEMMA 4. Let p be a prime with $p \mid d$, $p \nmid f$. Then there exists a unique class of H(d) representing p.

Proof. We first show that there is a class of H(d) representing p. If p is odd, as $p \mid d$ and $p \nmid f$, we have $p \mid\mid \Delta$ and $p \mid\mid d$. If $d \equiv 0 \pmod{4}$ then $[p, 0, -d/(4p)] \in H(d)$ represents p. If $d \equiv 1 \pmod{4}$, then the class $[p, p, (p^2 - d)/(4p)] \in H(d)$ represents p. If p = 2, as $2 \mid d$ and $2 \nmid f$, we have $2 \mid \Delta$ so that $4 \mid \Delta$ and $\Delta/4 \equiv 2$ or $3 \pmod{4}$. If $\Delta/4 \equiv 2 \pmod{4}$ then $d \equiv 8 \pmod{16}$ and $[2, 0, -d/8] \in H(d)$ represents 2. If $\Delta/4 \equiv 3 \pmod{4}$ then $d \equiv 12 \pmod{16}$ and $[2, 2, (4 - d)/8] \in H(d)$ represents 2.

We now show that the class of H(d) representing p is unique. Let K be a class representing p. As p is a prime any such representation of p by Kis proper so we have K = [p, b, c] with $b^2 - 4pc = d$. If p is odd and $d \equiv 0$ (mod 4) then $b \equiv 0 \pmod{2p}$ so that K = [p, 0, -d/(4p)]. If p is odd and $d \equiv 1 \pmod{4}$ then $b \equiv p \pmod{2p}$ so that $K = [p, p, (p^2 - d)/(4p)]$. If p = 2and $d \equiv 8 \pmod{16}$ then $b \equiv 0 \pmod{4}$ so that K = [2, 0, -d/8]. If p = 2and $d \equiv 12 \pmod{16}$ then $b \equiv 2 \pmod{4}$ so that K = [2, 2, (4 - d)/8].

As an immediate consequence of Lemma 4 we have

COROLLARY 1. Let p be a prime with $p \mid d, p \nmid f$. Then there exists a unique genus of G(d) representing p.

We denote the unique genus representing p by $\langle p \rangle$. As each prime p dividing U (see (6)) satisfies $p \mid d, p \nmid f$, we can define $\langle U \rangle \in G(d)$ by

$$\langle U \rangle = \prod_{p^{\alpha} \parallel U} \langle p \rangle^{\alpha}.$$

The mapping on G(d) given by $G \mapsto \langle U \rangle G$ is a bijection.

LEMMA 5. Let n be a positive integer and let $G \in G(d)$. Then n is represented by G if and only if n/U is represented by $\langle U \rangle G$.

Proof. Let p be a prime dividing d and n but not f. We show that $\langle p \rangle G \in G(d)$ represents n/p if and only if $G \in G(d)$ represents n. The assertion of the lemma then follows by repeatedly applying this result to all the primes p dividing U.

Suppose that G represents n. As $p \mid n$ we have $n = pn_1$ for some integer n_1 . Thus the genus $\langle p \rangle G$ represents $pn = p^2n_1$. Let K be a class in the genus $\langle p \rangle G$ which represents p^2n_1 . It is easy to show that K contains a form (a, bp, cp), where p divides neither a nor c (see [2, Lemma 7.1]). Thus there exist integers x and y such that

$$n_1p^2 = ax^2 + bpxy + cpy^2.$$

Clearly $p \mid x$. Then $p^2 \mid n_1 p^2 - ax^2 - bpxy = cpy^2$ so that as $p \nmid c$ we have $p \mid y$. Hence

P. Kaplan and K. S. Williams

$$n_1 = a(x/p)^2 + bp(x/p)(y/p) + cp(y/p)^2$$

so that n/p is represented by $[a, bp, cp] \in \langle p \rangle G$.

Suppose now that $\langle p \rangle G$ represents $n/p = n_1$. As $\langle p \rangle$ represents p, we see that $\langle p \rangle^2 G$ represents $pn_1 = n$. But $G_1^2 =$ principal genus for any genus G_1 so that $\langle p \rangle^2 G = G$ represents n.

3. Proof of Theorem. As *n* is represented by some form of discriminant *d*, we see by Lemma 2 that n/M^2 is represented by some form of discriminant d/M^2 and then by Lemma 5 that $n/(M^2Q)$ is represented by some form of discriminant d/M^2 . Also as *n* is represented by some form of discriminant *d*, we have Null $(n, d) = \emptyset$. Hence, by (10), we have $(n/(M^2Q), d/M^2) = 1$. Thus, by Lemma 1, we deduce that $g(n/(M^2Q), d/M^2) = 1$ so that

(18)
$$G(n/(M^2Q), d/M^2) = \{G_0\}$$

for some genus $G_0 \in G(d/M^2)$. Let $G_1 = \langle Q \rangle G_0 \in G(d/M^2)$. Clearly $\langle Q \rangle G_1 = \langle Q \rangle^2 G_0 = G_0$. Thus $n/(M^2Q)$ is represented by $\langle Q \rangle G_1$. Hence, by Lemma 5, we deduce that n/M^2 is represented by $G_1 \in G(d/M^2)$. Thus $G_1 \in G(n/M^2, d/M^2)$. Suppose $G_2 \ (\neq G_1) \in G(n/M^2, d/M^2)$. Then $G_2 \in G(d/M^2)$ represents n/M^2 . Hence, by Lemma 5, $n/(M^2Q)$ is represented by $\langle Q \rangle G_2 \in G(d/M^2)$, that is $\langle Q \rangle G_2 \in G(n/(M^2Q), d/M^2)$. Hence, by (18), we have $\langle Q \rangle G_2 = G_0$ so that $G_2 = \langle Q \rangle G_0 = G_1$, a contradiction. Hence

$$G(n/M^2, d/M^2) = \{G_1\}.$$

Then, by Lemma 3, we have

$$G(n,d) = \widetilde{\theta}_M^{-1}(G(n/M^2, d/M^2)) = \widetilde{\theta}_M^{-1}(\{G_1\}).$$

As $\tilde{\theta}_M : G(d) \to G(d/M^2)$ is a surjective homomorphism, there exists $G' \in G(d)$ such that $\theta_M(G') = G_1$. Hence

$$G(n,d) = \widetilde{\theta}_M^{-1}(\{G_1\}) = G' \ker \widetilde{\theta}_M$$

is a coset of the subgroup $\ker \tilde{\theta}_M$ of G(d). Since $G \in G(n,d)$ we have $G(n,d) = G \ker \tilde{\theta}_M$ as asserted.

Finally,

$$g(n,d) = |G(n,d)| = |G\ker\tilde{\theta}_M| = |\ker\tilde{\theta}_M| = \frac{|G(d)|}{|G(d/M^2)|} = 2^{t(d)-t(d/M^2)}.$$

As a special case of the Theorem, we have

COROLLARY 2. If the largest square dividing both n and f^2 is 1 then g(n,d) = 1.

Thus, in particular, if d is fundamental or (n, f) = 1 we have g(n, d) = 1.

4. Examples. We give three examples to illustrate the Theorem.

EXAMPLE 1. We take n = 8 and $d = -288 = -2^5 \cdot 3^2 \equiv 0 \pmod{32}$. Here

$$\omega(d) = 2, \quad \Delta = -8, \quad f = 6, \quad M = 2, \quad t(d) = \omega(d) = 2,$$

and

 $d/M^2 = -72 = -2^3 \cdot 3^2 \equiv 8 \pmod{16}, \quad t(d/M^2) = \omega(d/M^2) - 1 = 1.$ There are $2^{t(d)} = 2^2 = 4$ genera of discriminant -288. We have

$$G(-288) = \{I, A, B, AB\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2,$$

where

 $I = \{[1,0,72]\}, \quad A = \{[4,4,19]\}, \quad B = \{[8,0,9]\}, \quad AB = \{[8,8,11]\}, \text{ and }$

$$A^2 = B^2 = (AB)^2 = I.$$

There are $2^{t(d/M^2)} = 2^1 = 2$ genera of discriminant -72. We have $G(-72) = \{I_1, A_1\} \simeq \mathbb{Z}_2,$

where

$$I_1 = \{[1, 0, 18]\}, \quad A_1 = \{[2, 0, 9]\}, \quad A_1^2 = I_1.$$

The surjective homomorphism $\tilde{\theta}_2: G(-288) \to G(-72)$ is such that

$$\widetilde{\theta}_2(I) = \widetilde{\theta}_2(A) = I_1, \quad \widetilde{\theta}_2(B) = \widetilde{\theta}_2(AB) = A_1,$$

so that ker $\tilde{\theta}_2 = \{I, A\}$. As B represents 8 $(8 = 8 \cdot 1^2 + 9 \cdot 0^2)$ we have by the Theorem

$$G(8, -288) = B \ker \theta_2 = \{B, AB\}.$$

Hence g(8, -288) = 2.

EXAMPLE 2. We take $n = 640 = 2^7 \cdot 5$ and $d = -1984 = -2^6 \cdot 31 \equiv 0 \pmod{32}$. In this case we have

$$\omega(d) = 2, \quad \Delta = -31, \quad f = 8, \quad M = 8, \quad t(d) = \omega(d) = 2,$$

and

$$d/M^2 = -31 \equiv 1 \pmod{4}, \quad t(d/M^2) = \omega(d/M^2) - 1 = 0.$$

There are $2^{t(d)} = 2^2 = 4$ genera of discriminant -1984. We have

$$G(-1984) = \{I, A, B, AB\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2,$$

where

$$I = \{[1, 0, 496], [20, \pm 4, 25]\},\$$

$$A = \{[4, 4, 125], [5, \pm 4, 100]\},\$$

$$B = \{[16, 0, 31], [7, \pm 2, 71]\},\$$

$$AB = \{[16, 16, 35], [19, \pm 12, 28]\}.$$

As $2^{t(d/M^2)} = 2^0 = 1$ there is just one genus of discriminant -31. We have $G(-31) = \{I_1\},\$

where

$$I_1 = \{ [1, 1, 8] \}.$$

The surjective homomorphism $\tilde{\theta}_8 : G(-1984) \to G(-31)$ is such that $\tilde{\theta}_8(G) = I_1$ for all $G \in G(-1984)$ so that ker $\tilde{\theta}_8 = \{I, A, B, AB\}$. As I represents 640 (640 = $12^2 + 496 \cdot 1^2$) we have by the Theorem

$$G(640, -1984) = I \ker \theta_8 = \{I, A, B, AB\}.$$

Hence g(640, -1984) = 4.

EXAMPLE 3. We take $n = 32 = 2^5$ and $d = 960 = 2^6 \cdot 3 \cdot 5 \equiv 0 \pmod{32}$. Here we have

$$\omega(d) = 3, \quad \Delta = 60, \quad f = 4, \quad M = 4, \quad t(d) = \omega(d) = 3,$$

and

 $d/M^2 = 60 = 2^2 \cdot 3 \cdot 5 \equiv 12 \pmod{16}, \quad t(d/M^2) = \omega(d/M^2) - 1 = 2.$ There are $2^{t(d)} = 2^3 = 8$ genera of discriminant 960. We have

$$G(960) = \{I, A, B, C, AB, AC, BC, ABC\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2,$$

where

$$I = \{[1, 0, -240]\}, \qquad A = \{[-3, 0, 80]\}, \\B = \{[-1, 0, 240]\}, \qquad C = \{[4, 4, -59]\}, \\AB = \{[3, 0, -80]\}, \qquad AC = \{[-7, 6, 33]\}, \\BC = \{[-4, 4, 59]\}, \qquad ABC = \{[7, 6, -33]\}.$$

As $2^{t(d/M^2)} = 2^2 = 4$ there are four genera of discriminant 60. We have $G(60) = \{I_1, A_1, B_1, A_1B_1\},$

where

$$I_1 = \{ [1, 0, -15] \}, \qquad A_1 = \{ [-3, 0, 5] \}, \\B_1 = \{ [-1, 0, 15] \}, \qquad A_1 B_1 = \{ [3, 0, -5] \}.$$

The surjective homomorphism $\widetilde{\theta}_4: G(960) \to G(60)$ is given by

$$\widetilde{\theta}_4(A) = A_1, \quad \widetilde{\theta}_4(B) = B_1, \quad \widetilde{\theta}_4(C) = I_1,$$

so that ker $\tilde{\theta}_4 = \{I, C\}$. As A represents 32 $(32 = -3 \cdot 4^2 + 80 \cdot 1^2)$ we have by the Theorem

 $G(32,960) = A \ker \tilde{\theta}_4 = \{A, AC\}.$

Hence g(32, 960) = 2.

Acknowledgements. The authors would like to thank Habib Muzaffar of Carleton University for his help in checking and correcting the details

360

of this paper, Greg Martin of the University of Toronto whose question to the second author at the 2001 Seaway Number Theory Conference led to an improvement in our Theorem, and an unknown referee for valuable suggestions.

References

- [1] P. G. L. Dirichlet, Vorlesungen über Zahlentheorie, Chelsea, New York, 1968.
- [2] J. G. Huard, P. Kaplan and K. S. Williams, The Chowla-Selberg formula for genera, Acta Arith. 73 (1995), 271–301.
- [3] P. Kaplan and K. S. Williams, The distance between ideals in the orders of a real quadratic field, Enseign. Math. 36 (1990), 321–358.

Département de Mathématiques	Centre for Research in Algebra and Number Theory
Université de Nancy I	School of Mathematics and Statistics
54506 Vandœuvre-lès-Nancy, France	Carleton University
E-mail: pierre.kaplan@wanadoo.fr	Ottawa, Ontario K1S 5B6, Canada
	E-mail: williams@math.carleton.ca

Received on 12.1.2001 and in revised form on 23.7.2001 (3949)