ACTA ARITHMETICA
122.2 (2006)

On the number of representations of n by $ax^2 + bxy + cy^2$

by

ZHI-HONG SUN (Huaian) and KENNETH S. WILLIAMS (Ottawa)

1. Introduction. Let $\mathbb{N}$ and $\mathbb{Z}$ denote the sets of natural numbers and integers respectively. A nonsquare integer d with $d \equiv 0, 1 \pmod 4$ is called a *discriminant*. Let d be a discriminant, $n \in \mathbb{N}$ and $a, b, c \in \mathbb{Z}$ with $b^2 - 4ac = d$. If there exist integers x and y with $n = ax^2 + bxy + cy^2$, we say that the pair $\{x, y\}$ is a *representation of* n *by* $ax^2 + bxy + cy^2$. When $d < 0$, every representation $\{x, y\}$ is called *primary*. When $d > 0$, the representation $\{x, y\}$ is called *primary* if it satisfies

$$2ax + (b - \sqrt{d})y > 0, \qquad 1 \le \left| \frac{2ax + (b + \sqrt{d})y}{2ax + (b - \sqrt{d})y} \right| < \varepsilon(d)^2,$$

which is equivalent to

$$\frac{1}{\varepsilon(d)} < \frac{2ax + (b - \sqrt{d})y}{2\sqrt{n|a|}} \le 1,$$

where $\varepsilon(d) = (x_1 + y_1\sqrt{d})/2$ and (x_1, y_1) is the solution in positive integers to the equation $X^2 - dY^2 = 4$ for which $x_1 + y_1\sqrt{d}$ is least (see [D], [H, p. 282]). For $a, b, c \in \mathbb{Z}$ we denote the binary quadratic form $ax^2 + bxy + cy^2$ by (a, b, c), and the equivalence class containing the form (a, b, c) by $[a, b, c]$. Since (a, b, c) is a form, we use $\gcd(a, b, c)$ to denote the greatest common divisor of a, b, c. If $\gcd(a, b, c) = 1$, the form (a, b, c) is said to be *primitive*. It is proved in Section 3 that whichever form (a_1, b_1, c_1) is chosen from $[a, b, c]$ the number of primary representations of n by (a_1, b_1, c_1) is the same. Based on this fact we can define the number of representations of n by the class $[a, b, c]$ to be

$$R([a, b, c], n) = |\{\{x, y\} \mid n = ax^2 + bxy + cy^2,\ \{x, y\} \text{ is primary}\}|.$$

2000 *Mathematics Subject Classification*: Primary 11E16; Secondary 11R29, 11E25.

The first author was supported by Natural Sciences Foundation of Jiangsu Educational Office (02KJB110007), and the second author was supported by Natural Sciences and Engineering Research Council of Canada grant A-7233.

For a discriminant d the conductor of d is the largest positive integer $f = f(d)$ such that $d/f^2 \equiv 0, 1 \pmod 4$. If $f(d) = 1$, we say that d is a *fundamental discriminant*. Let $H(d)$ be the form class group consisting of classes of primitive, integral binary quadratic forms of discriminant d. In this paper, inspired by the work in [D], [H], [HKW], [KW1], [KW2], [KW3], [MW1] and [MW2], we consider the problem of giving explicit formulae for $R(K,n)$ $(K \in H(d))$. Let (n_1, n_2) denote the greatest common divisor of n_1 and n_2. In Section 2, we introduce and study the mapping

$$\varphi_{k,m} : [a, bkm, ckm^2] \to [ak, bk, c]$$

from $H(d)$ to $H(d/m^2)$, where $k, m \in \mathbb{N}$ with $k \mid \frac{d}{f^2}$, $4 \nmid k$, $m \mid f$ and $(k, f/m) = 1$. For $n \in \mathbb{N}$ and $S \subseteq H(d)$ we let

$$(1.1) \qquad R(S,n) = \sum_{K \in S} R(K,n), \qquad N(n,d) = R(H(d),n) = \sum_{K \in H(d)} R(K,n).$$

Suppose $K \in H(d)$ and that H is a subgroup of $H(d)$. On the basis of the properties of the mapping $\varphi_{k,m}$, in Section 3 we give reduction formulas for $R(K,n)$ and $R(KH,n)$, which reduce the evaluation of $R(K,n)$ and $R(KH,n)$ to the case $(n,d) = 1$.

In Section 4 we obtain a complete formula for $N(n,d)$. When $d < 0$, the formula improves the result given by Huard, Kaplan and Williams in [HKW]. As usual we set

$$(1.2) \qquad w(d) = \begin{cases} 1 & \text{if } d > 0, \\ 2 & \text{if } d < -4, \\ 4 & \text{if } d = -4, \\ 6 & \text{if } d = -3. \end{cases}$$

In Section 4 we also show that $N(n,d)/w(d)$ is a multiplicative function of n and give the Euler product for the Dirichlet series $\sum_{n=1}^{\infty} \frac{N(n,d)}{w(d)} n^{-s}$ $(\mathrm{Re}(s) > 1)$.

Let d be a discriminant and $K \in H(d)$. In Section 5 we give explicit formulas for $R(K, p^t)$, where p is a prime and $t \in \mathbb{N}$. Let $G(d) = H(d)/H^2(d)$ denote the group of genera, and let $\omega(d)$ denote the number of distinct prime divisors of d. It is well known that (see [Cox, pp. 52–54], [D] and [HKW]) $|G(d)| = 2^{t(d)}$, where

$$(1.3) \qquad t(d) = \begin{cases} \omega(d) & \text{if } d \equiv 0 \pmod{32}, \\ \omega(d) - 2 & \text{if } d \equiv 4 \pmod{16}, \\ \omega(d) - 1 & \text{otherwise.} \end{cases}$$

In Section 6, we give formulas for $R(G,n)$ when $G \in G(d)$. In particular, we show that $R(G,n) = 0$ or $N(n,d)/2^{t(d) - t(d/(n,f^2))}$.

Suppose $H(d)=\{A_1^{k_1}\cdots A_r^{k_r}\mid 0\le k_1<h_1,\dots,0\le k_r<h_r\}$, where $h_1\cdots h_r=h(d)$. For $n\in\mathbb{N}$ and $M=A_1^{m_1}\cdots A_r^{m_r}\in H(d)$ we define

$$F(M,n)=\frac{1}{w(d)}\sum_{\substack{0\le k_1<h_1\\ \cdots\\ 0\le k_r<h_r}}\cos 2\pi\left(\frac{k_1m_1}{h_1}+\dots+\frac{k_rm_r}{h_r}\right)\cdot R(A_1^{k_1}\cdots A_r^{k_r},n).$$

In Section 7 we show that $F(M,n)$ is a multiplicative function of n (see Theorem 7.2). For example, if $h(d)=2,3,4$ and $H(d)$ is cyclic with identity I and generator A, then

$$F(A,n)=\begin{cases}(R(I,n)-R(A,n))/w(d) & \text{if } h(d)=2,3,\\ (R(I,n)-R(A^2,n))/w(d) & \text{if } h(d)=4\end{cases}$$

is a multiplicative function of n. In Section 8, using the Chebyshev polynomial of the second kind we establish a reduction theorem for $F(M,n)$ (see Theorem 8.2), and determine $F(M,p^t)$, where p is a prime, $t\in\mathbb{N}$ and $M\in H(d)$ (see Theorems 8.1 and 8.4).

As applications of the multiplicative property of $F(M,n)$, in Sections 9, 10, 11 we obtain formulas for $F(M,n)$ and $R(K,n)$ ($K\in H(d)$) in the cases $h(d)=2,3,4$.

In addition to the above notation, we also use throughout this paper the following notation: $\left(\frac{a}{m}\right)$—the Kronecker symbol, $[x]$—the greatest integer not exceeding x, $\operatorname{ord}_p n$—the nonnegative integer α such that $p^\alpha\mid n$ but $p^{\alpha+1}\nmid n$ (that is $p^\alpha\parallel n$), $\mu(n)$—the Möbius function, $(a,b,c)\sim(a',b',c')$—the form (a,b,c) is equivalent to (a',b',c'), I—the principal class $\left[1,\frac{1-(-1)^d}{2},\frac14\left(\frac{1-(-1)^d}{2}-d\right)\right]$ in $H(d)$, $H^r(d)$—the set $\{K^r\mid K\in H(d)\}$, $\mathbb{Z}^2$—the set of all pairs $\{x,y\}$ ($x,y\in\mathbb{Z}$), $\operatorname{Ker}\varphi$—the kernel of φ, $R(K)$—the set of integers represented by the class $K\in H(d)$.

2. The mapping $\varphi_{k,m}$. Let d be a discriminant. Assume

(2.1) $\quad f=f(d),\quad d_0=d/f^2,\quad k,m\in\mathbb{N},\quad k\mid d_0,\quad 4\nmid k,\quad m\mid f,\quad (k,f/m)=1.$

In this section we introduce a useful map $\varphi_{k,m}$ from $H(d)$ to $H(d/m^2)$, which will be crucial in the study of $R(K,n)$ ($K\in H(d)$). For use later we investigate many properties of $\varphi_{k,m}$. Some special cases of $\varphi_{k,m}$ have been considered in [HKW], [KW1] and [KW2].

LEMMA 2.1. *Let d be a discriminant with conductor f, $d_0=d/f^2$ and $K\in H(d)$.*

(i) *For $M\in\mathbb{N}$ there exist integers a,b,c such that $K=[a,b,c]$ with $(a,M)=1$.*

(ii) *If $k,m,n\in\mathbb{N}$, $k\mid d_0$, $4\nmid k$ and $m\mid f$, then there exist integers a,b,c such that $K=[a,bkm,ckm^2]$ with $(a,kmn)=1$. Moreover, if $(k,f/m)=1$, the integer c can be chosen so that $(c,k)=1$.*

Proof. (i) is a known result. See Lemmas 2.25, 2.3 of [Cox] or [S, Lemma 3.1]. Now we consider (ii). Clearly $km \mid d$. By (i), $K = [a, b', c']$ with $a, b', c' \in \mathbb{Z}$ and $(a, kmn) = 1$. Since $b'^2 - 4ac' = d \equiv 0 \pmod{km}$ we see that $(2, km) \mid b'$ and so $(2a, km) \mid b'$. Thus, there are integers x, b such that $2ax + b' = bkm$. If $2 \nmid km$, clearly $b \equiv b' \equiv d \pmod 2$. If $2 \mid km$, then a is odd and $2a(x + km/2) + b' = (a + b)km$. Thus, as $b \not\equiv b + a \pmod 2$, we can always choose integers x and b such that $2ax + b' = bkm$ and b is even or odd as we require. For such integers x and b we have

$$K = [a, b', c'] = [a, 2ax + b', ax^2 + b'x + c'] = [a, bkm, ckm^2]$$

and $ckm^2 \in \mathbb{Z}$, where

$$c = \frac{b^2k - \frac{d}{km^2}}{4a} = \frac{b^2k - \frac{d_0}{k}\left(\frac{f}{m}\right)^2}{4a}.$$

Since $(a, km^2) = 1$ we see that $4 \mid (b^2k - d/(km^2))$ implies $c \in \mathbb{Z}$.

If $2 \nmid k$, by the above we may assume $b \equiv d/m^2 \pmod 2$. Since $b^2 \equiv 0, 1 \pmod 4$ and $d/m^2 = d_0(f/m)^2 \equiv 0, 1 \pmod 4$ we see that $b^2 \equiv d/m^2 \pmod 4$ and so $4 \mid \left(b^2k - \frac{d}{km^2}\right)$. Thus $c \in \mathbb{Z}$. If $2 \mid k$ and $k \equiv d/(km^2) \pmod 4$, we choose b so that b is odd, then $4 \mid \left(b^2k - \frac{d}{km^2}\right)$ and so $c \in \mathbb{Z}$. If $2 \mid k$ and $k \not\equiv d/(km^2) \pmod 4$, since $4 \nmid k$ we see that $d/(km^2) \not\equiv 2 \pmod 4$. But, $2 \mid k$ implies $2 \mid d_0$ and so $4 \mid d_0$. Thus $\frac{d}{km^2} = \frac{d_0}{k}\left(\frac{f}{m}\right)^2 \equiv 0 \pmod 2$. Hence $4 \mid \frac{d}{km^2}$. Now we choose b so that b is even. Then $4 \mid \left(b^2k - \frac{d}{km^2}\right)$ and so $c \in \mathbb{Z}$.

Now assume $(k, f/m) = 1$. Let $k_0 = k/(2, k)$. Clearly $2 \nmid k_0$ and $(k_0, d_0/k_0) = 1$. Thus

$$(4ac, k_0) = \left(b^2k - \frac{d_0}{k}\left(\frac{f}{m}\right)^2, k_0\right) = \left(\frac{d_0}{k}\left(\frac{f}{m}\right)^2, k_0\right) = 1$$

and hence $(c, k_0) = 1$. If k is even, we need to show that c is odd. Since $(a, km) = 1$ and $(k, f/m) = 1$ we see that a and f/m are odd. Thus noting that $d_0/4 \equiv 2, 3 \pmod 4$ we then obtain

$$\begin{aligned} c \equiv ac &= \frac{b^2k - d/(km^2)}{4} = \frac{b^2k_0 - d/(4k_0m^2)}{2} \\ &\equiv \frac{b^2 - d/(4m^2)}{2} \equiv \frac{b^2 - d_0/4}{2} \equiv 1 \pmod 2. \end{aligned}$$

Thus $(c, k) = 1$. This completes the proof.

Remark 2.1. We note that k is squarefree when $k \mid d_0$ and $4 \nmid k$. The special case $k = n = 1$ of Lemma 2.1(ii) was stated by Kaplan and Williams in [KW2, p. 355], and the case $m = n = 1$, $k =$ prime was proved by Kaplan and Williams in [KW1, p. 154].

Lemma 2.2. *Let $a,b,c\in\mathbb{Z}$ and $k,m,n\in\mathbb{N}$ with $(a,km)=1$ and $km^2\mid n$. If k is squarefree and $n=ax^2+bkmxy+ckm^2y^2$ for $x,y\in\mathbb{Z}$, then $km\mid x$.*

Proof. As $(2ax+bkmy)^2=4an+(b^2k-4ac)km^2y^2$ we see that $m\mid 2ax$ and so $\frac{m}{(2,m)}\mid x$. Hence $ax^2=n-bkmxy-ckm^2y^2\equiv 0 \pmod{\frac{m^2}{(2,m)}}$ and so $m\mid x$. Set $x_0=x/m$. By $n/m^2=ax_0^2+bkx_0y+cky^2$ we have $k\mid x_0^2$ and so $k\mid x_0$. This proves the lemma.

Lemma 2.3. *Let $a,b,c,a',b',c'\in\mathbb{Z}$, and let $k,m\in\mathbb{N}$ with $(a,km)=(a',km)=1$. If k is squarefree and $(a,bkm,ckm^2)\sim(a',b'km,c'km^2)$, then $(ak,bk,c)\sim(a'k,b'k,c')$.*

Proof. Since $(a,bkm,ckm^2)\sim(a',b'km,c'km^2)$ there exist $r,s,t,u\in\mathbb{Z}$ such that $ru-st=1$ and

$$a(rx+sy)^2+bkm(rx+sy)(tx+uy)+ckm^2(tx+uy)^2 = a'x^2+b'kmxy+c'km^2y^2.$$

This implies

$$ak(rx+s_0y)^2+bk(rx+s_0y)(t_0x+uy)+c(t_0x+uy)^2 = a'kx^2+b'kxy+c'y^2,$$

where $s_0=s/(km)$ and $t_0=kmt$. Since $c'km^2=as^2+bkmsu+ckm^2u^2$ we have $s_0\in\mathbb{Z}$ by Lemma 2.2. Thus the result follows.

In view of Lemmas 2.1 and 2.3 we introduce

Definition 2.1. Let d be a discriminant. Assume (2.1) holds. Then for any $K\in H(d)$ there exist $a,b,c\in\mathbb{Z}$ such that $K=[a,bkm,ckm^2]$ with $(a,km)=1$ and $(c,k)=1$. Define $\varphi_{k,m}(K)=[ak,bk,c]$. Note that any form equivalent to a primitive form is itself primitive. We see that $\varphi_{k,m}$ is a well defined mapping from $H(d)$ to $H(d/m^2)$.

By the definition, for any $[a,bm,cm^2]\in H(d)$ and $[a,bk,ck]\in H(d)$ with $(c,k)=1$ we have

$$\varphi_{1,m}([a,bm,cm^2])=[a,b,c],\qquad \varphi_{k,1}([a,bk,ck])=[ak,bk,c]$$

and

$$\varphi_{k,m}(K)=\varphi_{k,1}(\varphi_{1,m}(K))\quad\text{ for } K\in H(d).$$

Lemma 2.4 ([C, p. 246]). *Let (a_1,b_1,c_1) and (a_2,b_2,c_2) be two primitive integral binary quadratic forms of the same discriminant d, $t=\gcd(a_1,a_2,(b_1+b_2)/2)$, and let u,v,w be integers such that*

$$a_1u+a_2v+\frac{b_1+b_2}{2}\,w=t.$$

If $a_3 = a_1a_2/t^2$, $b_3 = b_2 + 2a_2\big(\frac{b_1-b_2}{2}v - c_2w\big)/t$ *and* $c_3 = (b_3^2 - d)/(4a_3)$, *then*

$$[a_1, b_1, c_1][a_2, b_2, c_2] = [a_3, b_3, c_3].$$

Theorem 2.1. *Let* d *be a discriminant with conductor* f. *Let* $m \in \mathbb{N}$ *and* $m \mid f$. *Then* $\varphi_{1,m}$ *is a surjective homomorphism from* $H(d)$ *to* $H(d/m^2)$. *Thus* $\mathrm{Ker}\,\varphi_{1,m}$ *is a subgroup of* $H(d)$ *and* $H(d/m^2) \cong H(d)/\mathrm{Ker}\,\varphi_{1,m}$.

Proof. For $A \in H(d/m^2)$, by Lemma 2.1(i) we may assume $A = [a, b, c]$ with $a, b, c \in \mathbb{Z}$ and $(a, m) = 1$. Clearly $[a, bm, cm^2] \in H(d)$ and $\varphi_{1,m}([a, bm, cm^2]) = A$. So $\varphi_{1,m}$ is onto.

Let $[a_1, b_1m, c_1m^2]$, $[a_2, b_2m, c_2m^2] \in H(d)$, $(a_1, m) = (a_2, m) = 1$ and $t = \gcd\big(a_1, a_2, \frac{b_1+b_2}{2}m\big) = \gcd\big(a_1, a_2, \frac{b_1+b_2}{2}\big)$. Let $u, v, w \in \mathbb{Z}$ be such that $a_1u + a_2v + \frac{b_1+b_2}{2}(mw) = t$. By Lemma 2.4 we have

$$[a_1, b_1m, c_1m^2][a_2, b_2m, c_2m^2] = [a_3, b_3m, c_3m^2],$$

where

$$a_3 = \frac{a_1a_2}{t^2}, \quad b_3 = b_2 + 2a_2\,\frac{v(b_1-b_2)/2 - c_2(mw)}{t}, \quad c_3 = \frac{b_3^2 - d/m^2}{4a_3}.$$

From this we see that $[a_1, b_1, c_1][a_2, b_2, c_2] = [a_3, b_3, c_3]$ by Lemma 2.4. Since $(a_1, m) = (a_2, m) = 1$ we have $(a_3, m) = 1$. Hence

$$\begin{aligned}\varphi_{1,m}&([a_1, b_1m, c_1m^2][a_2, b_2m, c_2m^2])\\ &= \varphi_{1,m}([a_3, b_3m, c_3m^2]) = [a_3, b_3, c_3] = [a_1, b_1, c_1][a_2, b_2, c_2]\\ &= \varphi_{1,m}([a_1, b_1m, c_1m^2])\varphi_{1,m}([a_2, b_2m, c_2m^2]).\end{aligned}$$

This shows that $\varphi_{1,m}$ is a homomorphism. Hence $\varphi_{1,m}$ is a surjective homomorphism from $H(d)$ to $H(d/m^2)$. Thus $\mathrm{Ker}\,\varphi_{1,m}$ is a subgroup of $H(d)$ and $H(d/m^2) \cong H(d)/\mathrm{Ker}\,\varphi_{1,m}$. This proves the theorem.

Remark 2.2. Theorem 2.1 was stated by Kaplan and Williams in [KW2, p. 355] as a consequence of known results on ideal classes. The above is a straightforward self-contained proof of this result. By Theorem 2.1 we have $h(d/m^2) = h(d)/|\mathrm{Ker}\,\varphi_{1,m}|$ and so $h(d/m^2) \mid h(d)$ for $m \mid f$.

Lemma 2.5. *Let* d *be a discriminant with conductor* f *and* $d_0 = d/f^2$. *Suppose* $k \in \mathbb{N}$, $k \mid d_0$, $4 \nmid k$ *and* $(k, f) = 1$. *For* $K_1, K_2 \in H(d)$ *we have*

$$\varphi_{k,1}(K_1)\varphi_{k,1}(K_2) = K_1K_2.$$

Proof. By Lemma 2.1(ii), for $i = 1, 2$ we may assume $K_i = [a_i, b_ik, c_ik]$ with $(a_i, k) = 1$. Clearly $(b_ik)^2 - 4a_ic_ik = d$. If $2 \nmid k$, then $b_i \equiv b_ik \equiv (b_ik)^2 \equiv d \pmod 2$. If $2 \mid k$, then $k \equiv 2 \pmod 4$, $2 \mid d_0$ and so $4 \mid d_0$. Thus $b_i \equiv b_i^2\big(\frac{k}{2}\big)^2 - a_ic_ik = \frac{d}{4} \pmod 2$. Hence we always have $b_1 \equiv d/(2, k)^2 \equiv b_2 \pmod 2$ and so $(b_1 \pm b_2)/2 \in \mathbb{Z}$.

Let $t=\gcd(a_1,a_2,(b_1+b_2)k/2)$, and let u,v,w be integers such that $a_1u+a_2v+\frac{b_1+b_2}{2}kw=t$. Set $a=a_1a_2/t^2$, $b=b_2k+2a_2\bigl(\frac{b_1-b_2}{2}kv-c_2kw\bigr)/t$ and $c=(b^2-d)/(4a)$. By Lemma 2.4 we have

$$K_1K_2=[a_1,b_1k,c_1k][a_2,b_2k,c_2k]=[a,b,c].$$

Let $t'=\gcd(a_1k,a_2k,(b_1k+b_2k)/2)$. Then clearly $t'=kt$. Since

$$a_1k\cdot u+a_2k\cdot v+\frac{b_1k+b_2k}{2}\cdot kw=t',\qquad a=\frac{a_1a_2}{t^2}=\frac{a_1k\cdot a_2k}{t'^2},$$

$$b=b_2k+2a_2\left(\frac{b_1-b_2}{2}\,kv-c_2kw\right)\Big/t=b_2k+2a_2k\left(\frac{b_1-b_2}{2}\,kv-c_2(kw)\right)\Big/t',$$

by Lemma 2.4 we also have

$$\varphi_{k,1}(K_1)\varphi_{k,1}(K_2)=[a_1k,b_1k,c_1][a_2k,b_2k,c_2]=[a,b,c].$$

Thus the result follows.

Theorem 2.2. *Let d be a discriminant with conductor f and $d_0=d/f^2$. Suppose $k\in\mathbb{N}$, $k\mid d_0$, $4\nmid k$ and $(k,f)=1$. For $K\in H(d)$ we have*

$$\varphi_{k,1}(K)=\begin{cases}\left[k,0,\dfrac{-d}{4k}\right]K & \text{if } 4k\mid d,\\[2ex] \left[k,k,\dfrac{k^2-d}{4k}\right]K & \text{if } 4k\nmid d.\end{cases}$$

Proof. For $a,b,c\in\mathbb{Z}$ with $(ac,k)=1$ and $[a,bk,ck]\in H(d)$ it is clear that

$$\begin{aligned}\varphi_{k,1}([a,bk,ck]^{-1})&=\varphi_{k,1}([a,-bk,ck])=[ak,-bk,c]\\&=[ak,bk,c]^{-1}=\varphi_{k,1}([a,bk,ck])^{-1}.\end{aligned}$$

Thus, by Lemma 2.1(ii), for $K\in H(d)$ we have $\varphi_{k,1}(K)^{-1}=\varphi_{k,1}(K^{-1})$ and hence $\varphi_{k,1}(I)^{-1}=\varphi_{k,1}(I)$, where I is the principal class in $H(d)$. Now applying Lemma 2.5 we have

$$\varphi_{k,1}(K)\varphi_{k,1}(I)=KI=K\quad\text{and so}\quad\varphi_{k,1}(K)=\varphi_{k,1}(I)K.$$

So we need only show that

$$\varphi_{k,1}(I)=\begin{cases}\left[k,0,\dfrac{-d}{4k}\right] & \text{if } 4k\mid d,\\[2ex] \left[k,k,\dfrac{k^2-d}{4k}\right] & \text{if } 4k\nmid d.\end{cases}$$

Since $k\mid d_0$, $4\nmid k$ and $(k,f)=1$ we know that k is a squarefree integer and so $(k/(2,k),d/k)=(k/(2,k),d_0f^2/k)=1$. If $2\mid k$, we must have $4\mid d_0$, $2\nmid f$ and $d_0/4\equiv 2,3 \pmod 4$. Now we prove the above assertion by considering the following four cases.

Case 1: $4 \mid d$ *and* $2 \nmid k$. In this case, $4k \mid d$ and $I = [1, 0, -d/4] = [1, 0, k(-d)/(4k)]$. Since $(k, -d/(4k)) = (k, d/k) = 1$ we see that $\varphi_{k,1}(I) = [k, 0, -d/(4k)]$.

Case 2: $8 \mid d$ *and* $2 \mid k$. In this case, $4k \mid d$ and $8 \mid d_0$. But $8 \mid d_0$ implies $2^3 \parallel d_0$. Hence $2^3 \parallel d$ and so $-d/(4k)$ is odd. As $(k, -d/(4k)) = (k/2, d/k) = 1$ we see that

$$\varphi_{k,1}(I) = \varphi_{k,1}([1, 0, k(-d)/(4k)]) = [k, 0, -d/(4k)].$$

Case 3: $2^2 \parallel d$ *and* $2 \mid k$. In this case, $4k \nmid d$, $2^2 \parallel d_0$ and so $d_0/4 \equiv 3 \pmod 4$. Thus

$$\frac{k^2-d}{4} = \left(\frac{k}{2}\right)^2 - \frac{d_0}{4} f^2 \equiv 1 - 3\cdot 1 \equiv 2 \pmod 4 \quad \text{and so} \quad \frac{k^2-d}{4k} \equiv 1 \pmod 2.$$

Hence $(k, (k^2-d)/(4k)) = (k/2, (k^2-d)/k) = (k/2, d/k) = 1$ and so

$$\begin{aligned}\varphi_{k,1}(I) &= \varphi_{k,1}([1, 0, -d/4]) = \varphi_{k,1}([1, k, k(k^2-d)/(4k)]) \\ &= [k, k, (k^2-d)/(4k)].\end{aligned}$$

Case 4: $d \equiv 1 \pmod 4$. In this case, $2 \nmid k$, $4k \nmid d$ and $(k, (k^2-d)/(4k)) = (k, (k^2-d)/k) = (k, d/k) = 1$. Thus

$$\begin{aligned}\varphi_{k,1}(I) &= \varphi_{k,1}([1, 1, (1-d)/4]) = \varphi_{k,1}([1, k, k(k^2-d)/(4k)]) \\ &= [k, k, (k^2-d)/(4k)].\end{aligned}$$

This completes the proof of the assertion and hence the theorem is proved.

Remark 2.3. From Theorem 2.2 we deduce that $\varphi_{k,1}$ is a bijection from $H(d)$ to $H(d)$. When k is a prime, this was stated and proved by Kaplan and Williams in [KW1].

Theorem 2.3. *Let d be a discriminant. Assume* (2.1) *holds. Then $\varphi_{k,m}$ is a surjective map from $H(d)$ to $H(d/m^2)$. Moreover*, *for $K, L \in H(d)$ we have*

$$\varphi_{k,m}(KL) = \varphi_{k,m}(K)\varphi_{1,m}(L).$$

Proof. We have already observed that $\varphi_{k,m}(K) = \varphi_{k,1}(\varphi_{1,m}(K))$. Since $\varphi_{1,m}$ is a surjective homomorphism and $\varphi_{k,1}$ is a bijection, we see that $\varphi_{k,m}$ is a surjective map from $H(d)$ to $H(d/m^2)$. Let

$$I_{k,m} = \begin{cases} \left[k, 0, \dfrac{-d/m^2}{4k}\right] & \text{if } 4k \mid \dfrac{d}{m^2}, \\[2ex] \left[k, k, \dfrac{k^2 - d/m^2}{4k}\right] & \text{if } 4k \nmid \dfrac{d}{m^2}. \end{cases} \tag{2.2}$$

From Theorem 2.2 we know that $\varphi_{k,1}(A) = I_{k,m}A$ for $A \in H(d/m^2)$. Recall that $\varphi_{1,m}$ is a homomorphism. Then we have

$$\begin{aligned}\varphi_{k,m}(KL) &= \varphi_{k,1}(\varphi_{1,m}(KL)) = I_{k,m}\varphi_{1,m}(KL) = I_{k,m}\varphi_{1,m}(K)\varphi_{1,m}(L) \\ &= \varphi_{k,1}(\varphi_{1,m}(K))\varphi_{1,m}(L) = \varphi_{k,m}(K)\varphi_{1,m}(L).\end{aligned}$$

This proves the theorem.

Now we are in a position to give

THEOREM 2.4. *Let d be a discriminant with conductor f and $d_0 = d/f^2$. Let $K \in H(d)$, $n \in \mathbb{N}$ and*

$$d_1 = \begin{cases} d_0 & \text{if } 4 \nmid d_0, \\ d_0/2 & \text{if } 2^2 \parallel d_0, \\ d_0/4 & \text{if } 2^3 \parallel d_0. \end{cases}$$

(i) *There exist integers a, b, c such that $K = [a, bd_1f, cd_1f^2]$ with $(a, dn) = 1$ and $(c, d_0) = 1$.*
(ii) *If $k \in \mathbb{N}$ and $k \mid \frac{d_1}{(d_1,f)}$, then there exist $a, b, c \in \mathbb{Z}$ such that $K = [ak, bkf, cf^2]$ with $(a, kfn) = (c, k) = 1$.*

Proof. Putting $k = d_1$ and $m = f$ in Lemma 2.1 gives (i). Now consider (ii). Suppose $k \in \mathbb{N}$ and $k \mid \frac{d_1}{(d_1,f)}$. Then $k \mid d_1$ and $(k, f) = 1$. Since $dm^2 = d_0(fm)^2$ for $m \in \mathbb{N}$, by Lemma 2.1 every class in $H(dm^2)$ is of the form $[a, bkfm, ck(fm)^2]$ with $a, b, c \in \mathbb{Z}$ and $(a, kfmn) = (c, k) = 1$. Since $\varphi_{k,m}$ is a surjective map and $\varphi_{k,m}([a, bkfm, ckf^2m^2]) = [ak, bkf, cf^2] \in H(d)$ we see that (ii) is true.

REMARK 2.4. Let d be a discriminant. Suppose that (2.1) holds. For $[a, bd_1f, cd_1f^2] \in H(d)$ with $(a, d) = 1$ and $(c, d_0) = 1$ we have

$$\varphi_{k,m}([a, bd_1f, cd_1f^2]) = [ak, bd_1f/m, cd_1f^2/(km^2)].$$

THEOREM 2.5. *Let d be a discriminant. Assume* (2.1) *holds. For $S \subseteq H(d)$ set $\varphi_{k,m}(S) = \{\varphi_{k,m}(A) \mid A \in S\}$. Let H be a subgroup of $H(d)$. Then*

(i) *$\varphi_{1,m}(H)$ is a subgroup of $H(d/m^2)$.*
(ii) *For $K \in H(d)$ we have $\varphi_{k,m}(KH) = \varphi_{k,m}(K)\varphi_{1,m}(H)$.*
(iii) *Suppose $M \in H(d/m^2)$. Then there are exactly $h(d)|\varphi_{1,m}(H)|/(h(d/m^2)|H|)$ distinct cosets $KH \in H(d)/H$ such that $\varphi_{k,m}(KH) = M\varphi_{1,m}(H)$. Moreover, if $K_0 \in H(d)$, $\varphi_{k,m}(K_0) = M$, $H_0 = H \cap \operatorname{Ker}\varphi_{1,m}$ and $\operatorname{Ker}\varphi_{1,m}/H_0 = \{A_1H_0, \dots, A_sH_0\}$, then all the distinct cosets $KH \in H(d)/H$ such that $\varphi_{k,m}(KH) = M\varphi_{1,m}(H)$ are $A_1K_0H, \dots, A_sK_0H$.*

Proof. Since $\varphi_{1,m}$ is a surjective homomorphism, using group theory we see that (i) is true.

Now we consider (ii). Suppose $K \in H(d)$. From Theorem 2.3 we see that

$$\begin{aligned}\varphi_{k,m}(KH) &= \{\varphi_{k,m}(KL) \mid L \in H\} = \{\varphi_{k,m}(K)\varphi_{1,m}(L) \mid L \in H\}\\ &= \varphi_{k,m}(K)\varphi_{1,m}(H).\end{aligned}$$

This proves (ii).

Finally we consider (iii). Suppose $M \in H(d/m^2)$. From Theorem 2.3 we know that $\varphi_{k,m}$ is a surjective map from $H(d)$ to $H(d/m^2)$. Thus there exists a class $K_0 \in H(d)$ such that $\varphi_{k,m}(K_0) = M$. Let $K \in H(d)$, $H' = \varphi_{1,m}(H)$, $H_0 = H \cap \operatorname{Ker}\varphi_{1,m}$ and $\operatorname{Ker}\varphi_{1,m}/H_0 = \{A_1H_0, \ldots, A_sH_0\}$, and let $I_{k,m} \in H(d/m^2)$ be given by (2.2). Applying Theorems 2.1–2.3 and (ii) we see that

$$\begin{aligned}
&\varphi_{k,m}(KH) = MH'\\
&\quad \Leftrightarrow\ \varphi_{k,m}(K)H' = MH' \ \Leftrightarrow\ \varphi_{k,m}(K)M^{-1} \in H'\\
&\quad \Leftrightarrow\ \varphi_{k,m}(K)\varphi_{k,m}(K_0)^{-1} \in H'\\
&\quad \Leftrightarrow\ I_{k,m}\varphi_{1,m}(K)(I_{k,m}\varphi_{1,m}(K_0))^{-1} \in H'\\
&\quad \Leftrightarrow\ \varphi_{1,m}(KK_0^{-1}) = \varphi_{1,m}(K)\varphi_{1,m}(K_0)^{-1} \in H'\\
&\quad \Leftrightarrow\ \varphi_{1,m}(KK_0^{-1}) = \varphi_{1,m}(L) \quad \text{for some } L \in H\\
&\quad \Leftrightarrow\ KK_0^{-1}L^{-1} \in \operatorname{Ker}\varphi_{1,m} \quad \text{for some } L \in H\\
&\quad \Leftrightarrow\ KK_0^{-1} \in H\operatorname{Ker}\varphi_{1,m} \ \Leftrightarrow\ K \in K_0H\operatorname{Ker}\varphi_{1,m}\\
&\quad \Leftrightarrow\ K \in AK_0H \quad \text{for some } A \in \operatorname{Ker}\varphi_{1,m}\\
&\quad \Leftrightarrow\ KH = AK_0H \quad \text{for some } A \in \operatorname{Ker}\varphi_{1,m}\\
&\quad \Leftrightarrow\ KH = A_iK_0H_0H = A_iK_0H \quad \text{for some } i \in \{1, \ldots, s\}.
\end{aligned}$$

For $i, j \in \{1, \ldots, s\}$ it is clear that

$$\begin{aligned}A_iK_0H = A_jK_0H \ &\Leftrightarrow\ (A_iK_0)(A_jK_0)^{-1} \in H \ \Leftrightarrow\ A_iA_j^{-1} \in H\\ &\Leftrightarrow\ A_iA_j^{-1} \in H_0 \ \Leftrightarrow\ A_iH_0 = A_jH_0 \ \Leftrightarrow\ i = j.\end{aligned}$$

Thus

$$\begin{aligned}(2.3)\qquad \{KH \mid KH \in H(d)/H,\ &\varphi_{k,m}(KH) = MH'\}\\ &= \{A_1K_0H, \ldots, A_sK_0H\}.\end{aligned}$$

Since $\varphi_{1,m}$ is a surjective homomorphism from $H(d)$ to $H(d/m^2)$, $\varphi_{1,m}$ induces a surjective homomorphism from H to $\varphi_{1,m}(H)$. Thus, by group theory we have

$$H(d)/\operatorname{Ker}\varphi_{1,m} \cong H(d/m^2) \quad \text{and} \quad H/(H \cap \operatorname{Ker}\varphi_{1,m}) \cong \varphi_{1,m}(H).$$

(That is $H/H_0 \cong H'$.) Thus

$$|\mathrm{Ker}\,\varphi_{1,m}| = h(d)/h(d/m^2), \qquad |H_0| = |H|/|H'|$$

and so

$$s = |\mathrm{Ker}\,\varphi_{1,m}/H_0| = \frac{|\mathrm{Ker}\,\varphi_{1,m}|}{|H_0|} = \frac{h(d)|H'|}{h(d/m^2)|H|}.$$

This completes the proof.

Taking $H = I$ in Theorem 2.5 we have

Corollary 2.1. *Let d be a discriminant. Assume* (2.1) *holds. For any given $M \in H(d/m^2)$, there are exactly $h(d)/h(d/m^2)$ classes K in $H(d)$ such that $\varphi_{k,m}(K) = M$. Moreover, if $K, K_0 \in H(d)$ and $\varphi_{k,m}(K_0) = M$, then $\varphi_{k,m}(K) = M$ if and only if $K = K_0 A$ for some $A \in \mathrm{Ker}\,\varphi_{1,m}$.*

Corollary 2.2. *Let d be a discriminant. Assume* (2.1) *holds. Let H be a subgroup of $H(d)$, $K \in H(d)$, $H_0 = H \cap \mathrm{Ker}\,\varphi_{1,m}$ and $\mathrm{Ker}\,\varphi_{1,m}/H_0 = \{H_0, A_2H_0, \ldots, A_sH_0\}$. Then*

$$\varphi_{k,m}(A_2KH) = \cdots = \varphi_{k,m}(A_sKH) = \varphi_{k,m}(KH).$$

For a discriminant d and $r \in \mathbb{N}$ recall that $H^r(d) = \{L^r \mid L \in H(d)\}$.

Lemma 2.6. *Let d be a discriminant with conductor f and $d_0 = d/f^2$. Let r be a nonnegative integer and $m \in \mathbb{N}$ with $m \mid f$. Then*

(i) *$\varphi_{1,m}(H^r(d)) = H^r(d/m^2)$.*

(ii) *Suppose $k \in \mathbb{N}$, $k \mid d_0$, $4 \nmid k$ and $(k, f/m) = 1$. Then for $K \in H(d)$ we have*

$$\varphi_{k,m}(KH^r(d)) = \varphi_{k,m}(K)H^r(d/m^2).$$

Proof. Recall that $\varphi_{1,m}$ is a surjective homomorphism from $H(d)$ to $H(d/m^2)$. Let $K \in H(d)$ and $M \in H(d/m^2)$ be such that $\varphi_{1,m}(K) = M$. Then clearly $\varphi_{1,m}(K^r) = \varphi_{1,m}(K)^r = M^r$. Since $K^r \in H^r(d)$ and $M^r \in H^r(d/m^2)$ we obtain (i). Combining (i) with Theorem 2.5(ii) yields (ii). So the lemma is proved.

From Theorem 2.5 and Lemma 2.6 we have

Theorem 2.6. *Let d be a discriminant. Assume* (2.1) *holds. Let r be a nonnegative integer and $M \in H(d/m^2)$. Then there are exactly $|H(d)/H^r(d)|/|H(d/m^2)/H^r(d/m^2)|$ distinct cosets $KH^r(d) \in H(d)/H^r(d)$ such that $\varphi_{k,m}(KH^r(d)) = MH^r(d/m^2)$. Moreover, if $K_0 \in H(d)$, $\varphi_{k,m}(K_0) = M$, $H_0 = H^r(d) \cap \mathrm{Ker}\,\varphi_{1,m}$ and $\mathrm{Ker}\,\varphi_{1,m}/H_0 = \{A_1H_0, \ldots, A_sH_0\}$, then all the distinct cosets $KH^r(d) \in H(d)/H^r(d)$ such that $\varphi_{k,m}(KH^r(d)) = MH^r(d/m^2)$ are $A_1K_0H^r(d), \ldots, A_sK_0H^r(d)$.*

Taking $r = 2$ in Lemma 2.6 and Theorem 2.6 and noting that $|H(d)/H^2(d)| = |G(d)| = 2^{t(d)}$ and $|H(d/m^2)/H^2(d/m^2)| = |G(d/m^2)| = 2^{t(d/m^2)}$ we obtain

COROLLARY 2.3. *Let d be a discriminant. Assume* (2.1) *holds. Then for any genus G of $H(d)$, $\varphi_{k,m}(G)$ is a genus of $H(d/m^2)$. For given $G' \in G(d/m^2)$ there are exactly $2^{t(d)-t(d/m^2)}$ genera $G \in G(d)$ such that $\varphi_{k,m}(G) = G'$. Moreover, if $\varphi_{k,m}(K_0) \in G'$ for $K_0 \in H(d)$, $H_0 = H^2(d) \cap \mathrm{Ker}\,\varphi_{1,m}$, and $\mathrm{Ker}\,\varphi_{1,m}/H_0 = \{A_1H_0, \dots, A_sH_0\}$, then all the genera G of $H(d)$ such that $\varphi_{k,m}(G) = G'$ are $A_1K_0H^2(d), \dots, A_sK_0H^2(d)$.*

3. Reduction theorems for $R(K, n)$ and $R(KH, n)$. Let d be a discriminant and $n \in \mathbb{N}$. Suppose $K \in H(d)$ and H is a subgroup of $H(d)$. Based on the results in Section 2, in this section we establish reduction theorems for $R(K, n)$ and $R(KH, n)$, which reduce the evaluation of $R(K, n)$ and $R(KH, n)$ to the case $(n, d) = 1$.

Let $n \in \mathbb{N}$ and $a, b, c \in \mathbb{Z}$. Suppose $n = ax^2 + bxy + cy^2$ with $x, y \in \mathbb{Z}$ and $(x, y) = 1$. As usual we say that $\{x, y\}$ is a *proper representation* of $n = ax^2 + bxy + cy^2$. It is well known that the general integral solution to $xs - yr = 1$ is $s = s_0 + ty$, $r = r_0 + tx$, where (s_0, r_0) is a fixed solution to $xs - yr = 1$ and $t \in \mathbb{Z}$. Clearly

$$(2ax + by)r + (bx + 2cy)s = (2ax + by)r_0 + (bx + 2cy)s_0 + 2nt.$$

Thus there exists a unique $t \in \mathbb{Z}$ such that $0 \le (2ax+by)r+(bx+2cy)s < 2n$. Hence there are two unique integers $r, s \in \mathbb{Z}$ such that $xs - yr = 1$ and $0 \le (2ax + by)r + (bx + 2cy)s < 2n$ (see [H, Theorem 4.1, p. 279]). For such r and s we let

$$\lambda(x, y; n) = (2ax + by)r + (bx + 2cy)s. \tag{3.1}$$

Then $\lambda(x, y; n)$ depends only on a, b, c, x, y, n and $0 \le \lambda(x, y; n) < 2n$.

LEMMA 3.1. *Let d be a discriminant and let $a, b, c \in \mathbb{Z}$ with $b^2-4ac = d$. Suppose $n \in \mathbb{N}$, $m \in \mathbb{Z}$ and $0 \le m < 2n$. Then there exists a proper representation $\{x, y\}$ of $n = ax^2+bxy+cy^2$ such that $\lambda(x, y; n) = m$ if and only if $m^2 \equiv d \pmod{4n}$ and $(n, m, (m^2 - d)/(4n)) \sim (a, b, c)$.*

Proof. If there exists a proper representation $\{x, y\}$ of $n = ax^2+bxy+cy^2$ such that $\lambda(x, y; n) = m$, then there are two unique integers r, s such that $xs - yr = 1$ and $m = (2ax + by)r + (bx + 2cy)s$. Thus

$$\begin{aligned} m^2 &= ((2ax + by)r + (bx + 2cy)s)^2 = 4n(ar^2 + brs + cs^2) + d(xs - yr)^2 \\ &= 4n(ar^2 + brs + cs^2) + d \equiv d \pmod{4n}. \end{aligned}$$

Since

$$\begin{aligned}(3.2)\qquad a(xX+rY)^2&+b(xX+rY)(yX+sY)+c(yX+sY)^2\\ &=(ax^2+bxy+cy^2)X^2+(2arx+bsx+bry+2csy)XY\\ &\quad+(ar^2+brs+cs^2)Y^2\\ &=nX^2+mXY+\frac{m^2-d}{4n}Y^2\end{aligned}$$

we see that $(n,m,(m^2-d)/(4n))\sim(a,b,c)$.

Conversely, if $m^2\equiv d \pmod{4n}$ and $(n,m,(m^2-d)/(4n))\sim(a,b,c)$, then there exist $x,y,r,s\in\mathbb{Z}$ with $xs-yr=1$ such that (3.2) holds. So $(x,y)=1$, $n=ax^2+bxy+cy^2$ and $m=2arx+bsx+bry+2csy=(2ax+by)r+(bx+2cy)s$. Thus $\{x,y\}$ is a proper representation of $n=ax^2+bxy+cy^2$ with $\lambda(x,y;n)=m$. So the lemma is proved.

LEMMA 3.2. *Let d be a discriminant and $a,b,c\in\mathbb{Z}$ with $b^2-4ac=d$. Suppose $n\in\mathbb{N}$, $m\in\mathbb{Z}$, $0\le m<2n$, $m^2\equiv d\pmod{4n}$, $(n,m,(m^2-d)/(4n))\sim(a,b,c)$. Then there are exactly $w(d)$ proper primary representations $\{x,y\}$ of $n=ax^2+bxy+cy^2$ such that $\lambda(x,y;n)=m$.*

Proof. By [H, Theorem 4.6, p. 282], if there is a proper primary representation $\{x_1,y_1\}$ of $n=ax^2+bxy+cy^2$ such that $\lambda(x_1,y_1;n)=m$, then there are exactly $w(d)$ proper primary representations $\{x,y\}$ of $n=ax^2+bxy+cy^2$ such that $\lambda(x,y;n)=m$ (Checking the proof of [H, Theorem 4.6], we do not need to assume that (a,b,c) is primitive.). Thus we need only show that there is a proper primary representation $\{x,y\}$ of $n=ax^2+bxy+cy^2$ such that $\lambda(x,y;n)=m$. By Lemma 3.1, there is a proper representation $\{x',y'\}$ of $n=ax^2+bxy+cy^2$ such that $\lambda(x',y';n)=m$. For $d<0$, every proper representation is a proper primary representation. So the result is true.

Now we assume $d>0$. From the proof of Lemma 3.1 there exist $x,y,r,s\in\mathbb{Z}$ such that $xs-yr=1$, $n=ax^2+bxy+cy^2$ and $m=(2ax+by)r+(bx+2cy)s=\lambda(x,y;n)$. Note that $(2ax+(b+\sqrt{d})y)(2ax+(b-\sqrt{d})y)=(2ax+by)^2-dy^2=4an\ne0$. Replacing (x,y,r,s) by $(-x,-y,-r,-s)$ if necessary we may suppose that $2ax+(b-\sqrt{d})y>0$. Since $\varepsilon(d)>1$ there is a unique integer k such that

$$\varepsilon(d)^{k-1}<\frac{2ax+(b-\sqrt{d})y}{2\sqrt{n|a|}}\le\varepsilon(d)^k.$$

Let $\varepsilon(d)^k=(t+u\sqrt{d})/2$. It is well known that $t^2-du^2=4$ (see [H, Theorem 4.4, pp. 281–282]). Now let

$$x'=\frac{x(t-bu)}{2}-cuy\quad\text{and}\quad y'=axu+\frac{y(t+bu)}{2}.$$

It is easily seen that $x',y'\in\mathbb{Z}$ and

$$2ax'+(b\pm\sqrt{d})y'=(2ax+(b\pm\sqrt{d})y)\varepsilon(d)^{\pm k}.$$

By [H, Theorem 4.2, p. 279], $\{x',y'\}$ is a proper representation of $n = ax^2+bxy+cy^2$ with $\lambda(x',y';n)=\lambda(x,y;n)=m$. We also have

$$\varepsilon(d)^{-1} < \frac{2ax'+(b-\sqrt{d})y'}{2\sqrt{n|a|}} = \frac{2ax+(b-\sqrt{d})y}{2\sqrt{n|a|}}\,\varepsilon(d)^{-k} \le 1.$$

Hence $\{x',y'\}$ is a proper primary representation of $n=ax^2+bxy+cy^2$ such that $\lambda(x',y';n)=m$. This finishes the proof.

Lemma 3.3 (Generalization of Möbius inversion formula). *Let $f(n)$ and $g(n)$ be defined for $n\in\mathbb{N}$. For $r\in\mathbb{N}$ we have the following inversion formula*:

$$f(n)=\sum_{m\in\mathbb{N},\,m^r\mid n} g\Big(\frac{n}{m^r}\Big)\ (n\ge 1) \ \Leftrightarrow\ g(n)=\sum_{m\in\mathbb{N},\,m^r\mid n}\mu(m)f\Big(\frac{n}{m^r}\Big)\ (n\ge 1),$$

where $\mu(n)$ is the Möbius function.

Proof. It is well known that

$$\sum_{m\mid n}\mu(m)=\begin{cases}1 & \text{if } n=1,\\ 0 & \text{if } n>1.\end{cases}$$

Thus, if $f(n)=\sum_{m^r\mid n} g\big(\frac{n}{m^r}\big)$ $(n\ge 1)$, then

$$\sum_{m^r\mid n}\mu(m)f\Big(\frac{n}{m^r}\Big)=\sum_{m^r\mid n}\mu(m)\sum_{d^r\mid \frac{n}{m^r}} g\Big(\frac{n}{d^rm^r}\Big)=\sum_{k^r\mid n}\sum_{dm=k}\mu(m)g\Big(\frac{n}{k^r}\Big)$$
$$=\sum_{k^r\mid n} g\Big(\frac{n}{k^r}\Big)\Big(\sum_{m\mid k}\mu(m)\Big)=g(n).$$

Similarly, if $g(n)=\sum_{m^r\mid n}\mu(m)f\big(\frac{n}{m^r}\big)$ $(n\ge 1)$, then

$$\sum_{m^r\mid n} g\Big(\frac{n}{m^r}\Big)=\sum_{m^r\mid n}\sum_{d^r\mid \frac{n}{m^r}}\mu(d)f\Big(\frac{n}{d^rm^r}\Big)=\sum_{k^r\mid n}\sum_{dm=k}\mu(d)f\Big(\frac{n}{k^r}\Big)$$
$$=\sum_{k^r\mid n} f\Big(\frac{n}{k^r}\Big)\Big(\sum_{d\mid k}\mu(d)\Big)=f(n).$$

So the lemma is proved.

Following [NZM] and [MW2] we introduce $H_{[a,b,c]}(n)$ as below.

Definition 3.1. Let d be a discriminant and $a,b,c\in\mathbb{Z}$ with $b^2-4ac=d$. For $n\in\mathbb{N}$ define $H_{[a,b,c]}(n)$ to be the number of integers m satisfying $0\le m<2n$, $m^2\equiv d \pmod{4n}$ and $(n,m,(m^2-d)/(4n))\in[a,b,c]$.

By this definition, $H_{[a,-b,c]}(n)$ is the number of integers x satisfying $0 \le x < 2n$, $x^2 \equiv d \pmod{4n}$ and $(n, x, (x^2-d)/(4n)) \in [a,-b,c]$. Since $(n, x, (x^2-d)/(4n)) \in [a,-b,c]$ if and only if $(n, -x, (x^2-d)/(4n)) \in [a,b,c]$, using the fact that $(A,B,C) \sim (A, 2A+B, A+B+C)$ we see that

$$\begin{aligned}
H_{[a,-b,c]}(n) &= |\{x \in \mathbb{Z} \mid 0 \le x < 2n,\ x^2 \equiv d \pmod{4n}, \\
&\qquad\qquad (n, -x, (x^2-d)/(4n)) \in [a,b,c]\}| \\
&= |\{m \in \mathbb{Z} \mid -2n < m \le 0,\ m^2 \equiv d \pmod{4n}, \\
&\qquad\qquad (n, m, (m^2-d)/(4n)) \in [a,b,c]\}| \\
&= |\{m \mid m+2n \in \{1,2,\dots,2n\},\ (m+2n)^2 \equiv d \pmod{4n}, \\
&\qquad\qquad (n, m+2n, ((m+2n)^2-d)/(4n)) \in [a,b,c]\}| \\
&= |\{x \mid x \in \{1,2,\dots,2n\},\ x^2 \equiv d \pmod{4n}, \\
&\qquad\qquad (n, x, (x^2-d)/(4n)) \in [a,b,c]\}| \\
&= H_{[a,b,c]}(n).
\end{aligned}$$

Thus for $K \in H(d)$ we have $H_K(n) = H_{K^{-1}}(n)$.

Definition 3.2. Suppose $a,b,c \in \mathbb{Z}$ and b^2-4ac is not a square. For $n \in \mathbb{N}$ we define $R'([a,b,c],n)$ to be the number of proper primary representations of $n = ax^2+bxy+cy^2$, and define $R([a,b,c],n)$ to be the number of primary representations of $n = ax^2+bxy+cy^2$.

By Lemmas 3.1 and 3.2, $R'([a,b,c],n)$ is well defined and $R'([a,b,c],n) = w(b^2-4ac)H_{[a,b,c]}(n)$. Now we show that $R([a,b,c],n)$ is well defined and reveal the connections among $R([a,b,c],n)$, $R'([a,b,c],n)$ and $H_{[a,b,c]}(n)$.

Theorem 3.1. *Let d be a discriminant, $n \in \mathbb{N}$ and $a,b,c \in \mathbb{Z}$ with $b^2-4ac = d$. Then*

$$R'([a,b,c],n) = w(d)H_{[a,b,c]}(n),$$

$$R([a,b,c],n) = \sum_{m\in\mathbb{N},\, m^2\mid n} R'\Big([a,b,c], \frac{n}{m^2}\Big) = w(d) \sum_{m\in\mathbb{N},\, m^2\mid n} H_{[a,b,c]}\Big(\frac{n}{m^2}\Big)$$

and

$$R'([a,b,c],n) = \sum_{m\in\mathbb{N},\, m^2\mid n} \mu(m) R\Big([a,b,c], \frac{n}{m^2}\Big).$$

Proof. From Lemmas 3.1, 3.2 and Definition 3.2 we see that

$$R'([a,b,c],n) = w(d)H_{[a,b,c]}(n).$$

Now we prove that

$$R([a,b,c],n) = \sum_{m^2\mid n} R'([a,b,c], n/m^2).$$

Clearly $\{x,y\}$ is a primary representation of $n = ax^2+bxy+cy^2$ with $(x,y)=m$ if and only if $\{x/m,y/m\}$ is a proper primary representation of $n/m^2 = aX^2+bXY+cY^2$. Thus

$$\begin{aligned} R([a,b,c],n) &= \sum_{m^2\mid n} |\{\{x,y\} \mid \{x,y\} \text{ is a primary representation} \\ &\qquad\qquad \text{of } n = ax^2+bxy+cy^2 \text{ with } (x,y)=m\}| \\ &= \sum_{m^2\mid n} |\{\{X,Y\} \mid \{X,Y\} \text{ is a proper primary representation} \\ &\qquad\qquad \text{of } n/m^2 = aX^2+bXY+cY^2\}| \\ &= \sum_{m^2\mid n} R'([a,b,c],n/m^2) = w(d)\sum_{m^2\mid n} H_{[a,b,c]}(n/m^2). \end{aligned}$$

This also shows that $R([a,b,c],n)$ is well defined by Definition 3.2. Now applying Lemma 3.3 in the case $r=2$ we deduce the remaining result. The proof is now complete.

Remark 3.1. Let d be a discriminant, $n \in \mathbb{N}$ and $a,b,c \in \mathbb{Z}$ with $b^2-4ac=d$. By the proof of Theorem 3.1, $R([a,b,c],n)$ is well defined. From Definition 3.1 and Theorem 3.1 we know that $H_{[a,b,c]}(n) \le 2n$ and so $R([a,b,c],n) \le w(d)\sum_{m^2\mid n} 2n/m^2$. Thus $R([a,b,c],n)$ is finite. Since $H_{[a,b,c]}(n) = H_{[a,-b,c]}(n)$ we see that $R([a,b,c],n) = R([a,-b,c],n)$ and $R'([a,b,c],n) = R'([a,-b,c],n)$ by Theorem 3.1. By Definition 3.1, it is easily seen that $H_{[ak,bk,ck]}(n) = H_{[a,b,c]}(n/k)$, where $k \in \mathbb{N}$ and $k\mid n$. From this and Theorem 3.1 we deduce $R'([ak,bk,ck],n) = R'([a,b,c],n/k)$ and $R([ak,bk,ck],n) = R([a,b,c],n/k)$. If $n = ax^2+bxy+cy^2$ with $x,y \in \mathbb{Z}$ and $(x,y)=m$, then $n/m^2 = ax_1^2+bx_1y_1+cy_1^2$ with $x_1,y_1 \in \mathbb{Z}$ and $(x_1,y_1)=1$. Using Lemma 3.1, Definition 3.1 and Theorem 3.1 we see that $H_{[a,b,c]}(n/m^2) > 0$ and so $R([a,b,c],n) > 0$. Thus n is represented by $ax^2+bxy+cy^2$ if and only if $n = ax^2+bxy+cy^2$ has a primary representation. When $d<0$ and $K \in H(d)$, the formula $R(K,n) = w(d)\sum_{m^2\mid n} H_K(n/m^2)$ has been given in [NZM, p. 174].

Theorem 3.2 (First Reduction Theorem for $R(K,n)$). *Let d be a discriminant with conductor f. Let $n \in \mathbb{N}$ and $K \in H(d)$. Then*

$$R(K,n) = \begin{cases} 0 & \text{if } (n,f^2) \text{ is not a square}, \\ R(\varphi_{1,m}(K), n/m^2) & \text{if } d<0 \text{ and } (n,f^2)=m^2, \\ \dfrac{\log\varepsilon(d)}{\log\varepsilon(d/m^2)} R(\varphi_{1,m}(K), n/m^2) & \text{if } d>0 \text{ and } (n,f^2)=m^2, \end{cases}$$

where $m \in \mathbb{N}$.

Proof. By Lemma 2.1 we may assume $K=[a,b,c]$ with $(a,f)=1$. If $R(K,n)>0$, then $n=ax^2+bxy+cy^2$ for some $x,y\in\mathbb{Z}$. Thus $4an=(2ax+by)^2-dy^2$. Since $(a,f)=1$ and $f^2\mid d$ we must have $(4n,f^2)=(4an,f^2)=((2ax+by)^2,f^2)=u^2$ for some $u\in\mathbb{Z}$. Hence (n,f^2) is a square when $\operatorname{ord}_2 n\neq \operatorname{ord}_2 f^2-1$. Now assume $\operatorname{ord}_2 n=\operatorname{ord}_2 f^2-1$. Then $2\mid f$, $4\mid d$, $2\mid b$ and $2\nmid a$. Set $d_0=d/f^2$, $f=2^\alpha f_0$ $(2\nmid f_0)$ and $n=2^{2\alpha-1}n_0$ $(2\nmid n_0)$. Note that $an=(ax+(b/2)y)^2-(f^2/4)d_0y^2$. Since $d_0\equiv 0,1 \pmod 4$ we see that $2\mid d_0$ implies $4\mid d_0$. Thus, if $2\mid d_0y$, then $4\mid d_0y^2$ and so

$$\begin{aligned}(n,f^2)&=(an,f^2)=((ax+by/2)^2-f^2d_0y^2/4,f^2)\\&=((ax+by/2)^2,f^2)=v^2\end{aligned}$$

for some $v\in\mathbb{Z}$. If $2\nmid d_0y$, then $d_0y^2\equiv 1 \pmod 4$ and so

$$\left(\frac{ax+by/2}{2^{\alpha-1}}\right)^2=\frac{an}{2^{2\alpha-2}}+\frac{f^2}{2^{2\alpha}}\,d_0y^2=2an_0+d_0f_0^2y^2\equiv 2+1=3 \pmod 4.$$

This is impossible. Thus (n,f^2) is always a square. Therefore, $R(K,n)=0$ when (n,f^2) is not a square.

Now suppose $(n,f^2)=m^2$ for some $m\in\mathbb{N}$. Then $m\mid f$ and $m^2\mid n$. By Lemma 2.1 we may suppose $K=[a,bm,cm^2]$ with $a,b,c\in\mathbb{Z}$ and $(a,m)=1$. If $R(K,n)>0$, then $n=ax^2+bmxy+cm^2y^2$ for some $x,y\in\mathbb{Z}$. By Lemma 2.2, we have $m\mid x$. Thus $n/m^2=aX^2+bXy+cy^2$ for $X=x/m\in\mathbb{Z}$ and $y\in\mathbb{Z}$. Conversely, if $n/m^2=aX^2+bXy+cy^2$ for some $X,y\in\mathbb{Z}$, then $\{mX,y\}$ is a solution to $n=ax^2+bmxy+cm^2y^2$. Thus for $d<0$ we have

$$R(K,n)=R([a,bm,cm^2],n)=R([a,b,c],n/m^2)=R(\varphi_{1,m}(K),n/m^2).$$

Now we assume $d>0$. By the above,

$$\begin{aligned}&\{x,y\}\text{ is a primary representation of } n=ax^2+bmxy+cm^2y^2\\&\quad\Leftrightarrow\ n=ax^2+bmxy+cm^2y^2,\ x,y\in\mathbb{Z},\ \frac{1}{\varepsilon(d)}<\frac{2ax+(bm-\sqrt{d})y}{2\sqrt{n|a|}}\le 1\\&\quad\Leftrightarrow\ \frac{n}{m^2}=aX^2+bXy+cy^2,\ X=\frac{x}{m}\in\mathbb{Z},\ y\in\mathbb{Z},\\&\qquad\qquad\frac{1}{\varepsilon(d)}<\frac{2aX+(b-\sqrt{d/m^2})y}{2\sqrt{n|a|/m^2}}\le 1.\end{aligned}$$

Suppose $\varepsilon(d)=(x_1+y_1\sqrt{d})/2$ and $D=d/m^2$. Then $x_1^2-D(my_1)^2=4$. Thus from [H, Theorem 4.4, p. 281] we know that $\varepsilon(d)=(x_1+my_1\sqrt{D})/2=\pm\varepsilon(D)^r$ for some $r\in\mathbb{Z}$. As $\varepsilon(d),\varepsilon(D)>1$ we must have $\varepsilon(d)=\varepsilon(D)^r$ for some $r\in\mathbb{N}$. Clearly

$$r=\log\varepsilon(d)/\log\varepsilon(D)\quad\text{and}\quad \varepsilon(d)^{-1}=\varepsilon(D)^{-r}.$$

Thus, applying the above we obtain

$$\begin{aligned}R(K,n) &= \Bigg|\Bigg\{\{X,Y\}\in\mathbb{Z}^2\ \Bigg|\ \frac{n}{m^2}=aX^2+bXY+cY^2,\\ &\qquad\qquad \varepsilon(D)^{-r}<\frac{2aX+(b-\sqrt{D})Y}{2\sqrt{n|a|/m^2}}\le 1\Bigg\}\Bigg|\\ &= \sum_{s=0}^{r-1}\Bigg|\Bigg\{\{X,Y\}\in\mathbb{Z}^2\ \Bigg|\ \frac{n}{m^2}=aX^2+bXY+cY^2,\\ &\qquad\qquad \varepsilon(D)^{-s-1}<\frac{2aX+(b-\sqrt{D})Y}{2\sqrt{n|a|/m^2}}\le \varepsilon(D)^{-s}\Bigg\}\Bigg|.\end{aligned}$$

For $s\in\{0,1,\dots,r-1\}$ let $\varepsilon(D)^s=(t_s+u_s\sqrt{D})/2$. Then $t_s^2-Du_s^2=4$ and $t_s\equiv Du_s\equiv bu_s \pmod 2$. Recall that $b^2-4ac=D$. Set

$$\begin{pmatrix}x\\ y\end{pmatrix}=\begin{pmatrix}(t_s+bu_s)/2 & cu_s\\ -au_s & (t_s-bu_s)/2\end{pmatrix}\begin{pmatrix}X\\ Y\end{pmatrix}.$$

We then see that

$$\begin{pmatrix}X\\ Y\end{pmatrix}=\begin{pmatrix}(t_s-bu_s)/2 & -cu_s\\ au_s & (t_s+bu_s)/2\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix}$$

and

$$2ax+(b\pm\sqrt{D})y=\frac{t_s\mp u_s\sqrt{D}}{2}\,(2aX+(b\pm\sqrt{D})Y).$$

Thus

$$\begin{aligned}4a(ax^2+bxy+cy^2)&=(2ax+(b+\sqrt{D})y)(2ax+(b-\sqrt{D})y)\\ &=\frac{t_s^2-Du_s^2}{4}\,(2aX+(b+\sqrt{D})Y)(2aX+(b-\sqrt{D})Y)\\ &=4a(aX^2+bXY+cY^2).\end{aligned}$$

Since $b^2-4ac=D$ is not a square we see that $a\ne 0$ and hence

$$ax^2+bxy+cy^2=aX^2+bXY+cY^2.$$

Now from all the above we derive that

$$\begin{aligned}R(K,n)&=\sum_{s=0}^{r-1}\Bigg|\Bigg\{\{X,Y\}\in\mathbb{Z}^2\ \Bigg|\ \frac{n}{m^2}=aX^2+bXY+cY^2,\\ &\qquad\qquad \varepsilon(D)^{-1}<\frac{2aX+(b-\sqrt{D})Y}{2\sqrt{n|a|/m^2}}\cdot\frac{t_s+u_s\sqrt{D}}{2}\le 1\Bigg\}\Bigg|\\ &=\sum_{s=0}^{r-1}\Bigg|\Bigg\{\{x,y\}\in\mathbb{Z}^2\ \Bigg|\ \frac{n}{m^2}=ax^2+bxy+cy^2,\\ &\qquad\qquad \varepsilon(D)^{-1}<\frac{2ax+(b-\sqrt{D})y}{2\sqrt{n|a|/m^2}}\le 1\Bigg\}\Bigg|\end{aligned}$$

$$= r|\{\{x,y\} \mid \{x,y\} \text{ is a primary representation of } n/m^2 = ax^2+bxy+cy^2\}|$$
$$= rR\left([a,b,c], \frac{n}{m^2}\right) = \frac{\log\varepsilon(d)}{\log\varepsilon(D)} R\left(\varphi_{1,m}(K), \frac{n}{m^2}\right).$$

This finishes the proof.

REMARK 3.2. Let d be a discriminant with conductor f. If $(n,f^2)=p^2$ for some prime p, the reduction formula in Theorem 3.2 has been given in [HKW, p. 286] ($d<0$) and [MW1, p. 35] ($d>0$).

From Theorems 2.1 and 3.2 we have

COROLLARY 3.1. *Let d be a discriminant with conductor f and $n \in \mathbb{N}$. If $(n,f^2)=m^2$ for $m\in\mathbb{N}$, $K,L\in H(d)$ and $L\in \operatorname{Ker}\varphi_{1,m}$, then*

$$R(K,n) = R(KL,n).$$

LEMMA 3.4. *Let d be a discriminant. Let $k\in\mathbb{N}$ be squarefree. Let $a,b,c\in\mathbb{Z}$ with $(a,k)=1$ and $(bk)^2-4ack=d$. Suppose $n\in\mathbb{N}$ with $k\mid n$. Then*

$$R([a,bk,ck],n) = R([ak,bk,c],n/k).$$

Furthermore, if $(c,k)=1$ and $k^2\mid n$, then

$$R([a,bk,ck],n) = R([a,bk,ck],n/k^2).$$

Proof. If $n = ax^2+bkxy+cky^2$ for some $x,y\in\mathbb{Z}$, then $k\mid x$ by Lemma 2.2. Set $x=kX$. We then have $n = ak^2X^2+bk^2Xy+cky^2$ and so $n/k = akX^2+bkXy+cy^2$. Conversely, if $n/k = akX^2+bkXy+cy^2$ for some $X,y\in\mathbb{Z}$, then $n=ax^2+bkxy+cky^2$ for integers $x=kX$ and y. Thus $R([a,bk,ck],n) = R([ak,bk,c],n/k)$ for $d<0$. If $d>0$, $n=ax^2+bkxy+cky^2$ $(x,y\in\mathbb{Z})$ and $x=kX$, from the above we see that

$\{x,y\}$ is a primary representation of $n=ax^2+bkxy+cky^2$

$$\Leftrightarrow\ \varepsilon(d)^{-1} < \frac{2ax+(bk-\sqrt{d})y}{2\sqrt{n|a|}} \le 1$$

$$\Leftrightarrow\ \varepsilon(d)^{-1} < \frac{2akX+(bk-\sqrt{d})y}{2\sqrt{|ak|n/k}} \le 1$$

$\Leftrightarrow\ \{X,y\}$ is a primary representation of $n/k = akX^2+bkXy+cY^2$.

Thus we also have $R([a,bk,ck],n) = R([ak,bk,c],n/k)$.

If $(c,k)=1$ and $k^2\mid n$, applying the above we see that

$$\begin{aligned} R([a,bk,ck],n) &= R([ak,bk,c],n/k) = R([c,-bk,ak],n/k) \\ &= R([ck,-bk,a],n/k^2) = R([a,bk,ck],n/k^2). \end{aligned}$$

This completes the proof.

REMARK 3.3. When k is a prime and $\gcd(a, bk, ck) = (c, k) = 1$, the first formula in Lemma 3.4 is known. See [HKW, Lemma 7.2] ($d < 0$) and [MW1, Lemma 10] ($d > 0$).

THEOREM 3.3 (Second Reduction Theorem for $R(K, n)$). *Let d be a discriminant with conductor f. Let $d_0 = d/f^2$ and $n \in \mathbb{N}$. Let k be the product of distinct prime divisors p of n such that $p \mid d_0$, $p \nmid f$ and $2 \nmid \operatorname{ord}_p n$, and let n_0 be the product of all prime divisors p of n such that $p \nmid d_0$ or $p \mid f$. Then for $K \in H(d)$ we have*

$$R(K, n) = R(\varphi_{k,1}(K), n_0).$$

Proof. Let $m \in \mathbb{N}$ and $K \in H(d)$. If p is a prime such that $p \mid d_0$, $p \nmid f$ and $p^2 \mid m$, by Lemma 2.1 we may assume $K = [a, bp, cp]$ with $a, b, c \in \mathbb{Z}$ and $p \nmid ac$. Thus applying Lemma 3.4 we see that

$$R(K, m) = R(K, m/p^2) = \cdots = R(K, m/p^{2[\frac{\operatorname{ord}_p m}{2}]}).$$

As

$$n = n_0 \prod_{p \mid d_0,\, p \nmid f} p^{\operatorname{ord}_p n} = k n_0 \prod_{p \mid d_0,\, p \nmid f} p^{2[\frac{\operatorname{ord}_p n}{2}]},$$

by the above we obtain $R(K, n) = R(K, kn_0)$. Since $k \mid d_0$, $(k, f) = 1$ and $4 \nmid k$, by appealing to Lemmas 2.1 and 3.4 again we find $R(K, kn_0) = R(\varphi_{k,1}(K), n_0)$. Thus the result follows.

Combining Theorems 3.2 and 3.3 we obtain

THEOREM 3.4 (Third Reduction Theorem for $R(K, n)$). *Let d be a discriminant with conductor f and $d_0 = d/f^2$. Let $n \in \mathbb{N}$ and $K \in H(d)$. If (n, f^2) is not a square, then $R(K, n) = 0$. If $(n, f^2) = m^2$ for $m \in \mathbb{N}$, setting*

$$k = \prod_{p \mid d_0,\, 2 \nmid \operatorname{ord}_p n} p \quad \text{and} \quad n' = \prod_{p \nmid d_0} p^{\operatorname{ord}_p (n/m^2)},$$

where p runs over all distinct prime divisors of n/m^2, we then have

$$R(K, n) = \begin{cases} R(\varphi_{k,m}(K), n') & \text{if } d < 0, \\ \dfrac{\log \varepsilon(d)}{\log \varepsilon(d/m^2)} R(\varphi_{k,m}(K), n') & \text{if } d > 0. \end{cases}$$

Proof. By Theorem 3.2 we need only consider the case $(n, f^2) = m^2$ for $m \in \mathbb{N}$. Let p be a prime dividing n/m^2. Then $p \nmid \frac{f}{m}$ since $\left(\frac{n}{m^2}, \frac{f^2}{m^2}\right) = 1$. Note that $d/m^2 = d_0(f/m)^2$. By Theorem 3.3 we have $R(\varphi_{1,m}(K), n/m^2) = R(\varphi_{k,1}(\varphi_{1,m}(K)), n')$. This together with Theorem 3.2 and the fact that $\varphi_{k,m}(K) = \varphi_{k,1}(\varphi_{1,m}(K))$ yields the result.

REMARK 3.4. Since $\varphi_{k,m}(K)\in H(d/m^2)$ and $(n',d/m^2)=(n',d_0f^2/m^2)=1$, using the reduction theorems we need only study $R(K,n)$ on the condition that $(n,d)=1$.

LEMMA 3.5. *Let d be a discriminant with conductor f. If $m\in\mathbb{N}$ and $m\mid f$, then*

$$m\prod_{p\mid m}\left(1-\frac{1}{p}\left(\frac{d/m^2}{p}\right)\right)=\begin{cases}\dfrac{h(d)w(d/m^2)}{h(d/m^2)w(d)} & \text{if } d<0,\\[2mm] \dfrac{h(d)\log\varepsilon(d)}{h(d/m^2)\log\varepsilon(d/m^2)} & \text{if } d>0,\end{cases}$$

where p runs over all distinct prime divisors of m.

Proof. Set $d_0=d/f^2$. Then clearly $d/m^2=d_0(f/m)^2$ is a discriminant with conductor f/m. From Dirichlet's class number formula (see [H, Theorem 10.1]) we know that

$$h(d)=\begin{cases}\dfrac{w(d)\sqrt{-d}}{2\pi}K(d) & \text{if } d<0,\\[2mm] \dfrac{\sqrt{d}}{\log\varepsilon(d)}K(d) & \text{if } d>0,\end{cases}$$

where $K(d)=\sum_{n=1}^{\infty}\frac{1}{n}\left(\frac{d}{n}\right)$. By [H, Theorem 11.2] we also have

$$K(d)=K(d_0)\prod_{p\mid f}\left(1-\frac{1}{p}\left(\frac{d_0}{p}\right)\right),$$

where p runs over all distinct prime divisors of f. Thus

$$\begin{aligned}f\prod_{p\mid f}\left(1-\frac{1}{p}\left(\frac{d_0}{p}\right)\right)&=\frac{fK(d)}{K(d_0)}\\ &=\begin{cases}\dfrac{2\pi fh(d)/(w(d)\sqrt{-d})}{2\pi h(d_0)/(w(d_0)\sqrt{-d_0})}=\dfrac{h(d)w(d_0)}{h(d_0)w(d)} & \text{if } d<0,\\[2mm] \dfrac{fh(d)\log\varepsilon(d)/\sqrt{d}}{h(d_0)\log\varepsilon(d_0)/\sqrt{d_0}}=\dfrac{h(d)\log\varepsilon(d)}{h(d_0)\log\varepsilon(d_0)} & \text{if } d>0.\end{cases}\end{aligned}$$

Applying this formula to the discriminant $d/m^2=d_0(f/m)^2$ we obtain

$$\frac{f}{m}\prod_{p\mid\frac{f}{m}}\left(1-\frac{1}{p}\left(\frac{d_0}{p}\right)\right)=\frac{fK(d/m^2)}{mK(d_0)}=\begin{cases}\dfrac{h(d/m^2)w(d_0)}{h(d_0)w(d/m^2)} & \text{if } d<0,\\[2mm] \dfrac{h(d/m^2)\log\varepsilon(d/m^2)}{h(d_0)\log\varepsilon(d_0)} & \text{if } d>0.\end{cases}$$

Comparing the two formulas we deduce that

$$m\prod_{p\mid f,\,p\nmid\frac{f}{m}}\Big(1-\frac{1}{p}\Big(\frac{d_0}{p}\Big)\Big)=\frac{f\prod_{p\mid f}\big(1-\frac{1}{p}\big(\frac{d_0}{p}\big)\big)}{\frac{f}{m}\prod_{p\mid\frac{f}{m}}\big(1-\frac{1}{p}\big(\frac{d_0}{p}\big)\big)}$$

$$=\begin{cases}\dfrac{h(d)w(d/m^2)}{h(d/m^2)w(d)} & \text{if } d<0,\\[2mm] \dfrac{h(d)\log\varepsilon(d)}{h(d/m^2)\log\varepsilon(d/m^2)} & \text{if } d>0.\end{cases}$$

To see the result, we note that

$$\prod_{p\mid m}\Big(1-\frac{1}{p}\Big(\frac{d/m^2}{p}\Big)\Big)=\prod_{p\mid m,\,p\nmid\frac{f}{m}}\Big(1-\frac{1}{p}\Big(\frac{d_0}{p}\Big)\Big)=\prod_{p\mid f,\,p\nmid\frac{f}{m}}\Big(1-\frac{1}{p}\Big(\frac{d_0}{p}\Big)\Big).$$

Remark 3.5. Lemma 3.5 is equivalent to a result given in [Coh, p. 217]. When $d<0$ and $m=f$, the formula can be found in [C, p. 233].

Theorem 3.5 (Reduction Theorem for $R(KH,n)$). *Let d be a discriminant with conductor f and $d_0=d/f^2$. Let H be a subgroup of $H(d)$, $K\in H(d)$ and $n\in\mathbb{N}$. If (n,f^2) is not a square, then $R(KH,n)=0$. If $(n,f^2)=m^2$ for $m\in\mathbb{N}$, and if k and n' are given by*

$$k=\prod_{p\mid d_0,\,2\nmid\operatorname{ord}_p n}p\quad\textit{and}\quad n'=\prod_{p\nmid d_0}p^{\operatorname{ord}_p(n/m^2)},$$

where p runs over all distinct prime divisors of n/m^2, then

$$\frac{R(KH,n)}{w(d)}=m\prod_{p\mid m}\Big(1-\frac{1}{p}\Big(\frac{d/m^2}{p}\Big)\Big)\cdot\frac{|H(d/m^2)/H'|}{|H(d)/H|}\cdot\frac{R(\varphi_{k,m}(K)H',n')}{w(d/m^2)},$$

where $H'=\varphi_{1,m}(H)=\{\varphi_{1,m}(L)\mid L\in H\}$ and p runs over all distinct prime divisors of m.

Proof. If (n,f^2) is not a square, then $R(L,n)=0$ for any $L\in H(d)$ and thus $R(KH,n)=0$. Now assume $(n,f^2)=m^2$ for $m\in\mathbb{N}$. Let $H_0=H\cap\operatorname{Ker}\varphi_{1,m}$ and $H/H_0=\{L_1H_0,\dots,L_rH_0\}$. Since $\varphi_{1,m}$ is a homomorphism, it is easy to see that $\varphi_{1,m}(H)=\{\varphi_{1,m}(L_1),\dots,\varphi_{1,m}(L_r)\}$ and thus

(3.3) $$|\varphi_{1,m}(H)|=r=|H/H_0|.$$

Set

(3.4) $$c(d,m)=\begin{cases}1 & \text{if } d<0,\\ \dfrac{\log\varepsilon(d)}{\log\varepsilon(d/m^2)} & \text{if } d>0.\end{cases}$$

Using Theorems 2.3, 3.4 and (3.3) we see that

$$\begin{aligned}
R(KH,n) &= \sum_{L\in H} R(KL,n) = c(d,m)\sum_{L\in H} R(\varphi_{k,m}(KL),n')\\
&= c(d,m)\sum_{L\in H} R(\varphi_{k,m}(K)\varphi_{1,m}(L),n')\\
&= c(d,m)\sum_{i=1}^{r}\sum_{L\in L_iH_0} R(\varphi_{k,m}(K)\varphi_{1,m}(L),n')\\
&= c(d,m)\sum_{i=1}^{r}|H_0|R(\varphi_{k,m}(K)\varphi_{1,m}(L_i),n')\\
&= c(d,m)|H_0|R(\varphi_{k,m}(K)\varphi_{1,m}(H),n')\\
&= \frac{c(d,m)|H|}{|\varphi_{1,m}(H)|}R(\varphi_{k,m}(K)\varphi_{1,m}(H),n').
\end{aligned}$$

As $H' = \varphi_{1,m}(H)$ is a subgroup of $H(d/m^2)$, applying Lemma 3.5 we have

$$\begin{aligned}
\frac{c(d,m)|H|}{|H'|} &= \frac{c(d,m)h(d)}{h(d/m^2)}\cdot\frac{|H(d/m^2)/H'|}{|H(d)/H|}\\
&= m\prod_{p|m}\left(1-\frac{1}{p}\left(\frac{d/m^2}{p}\right)\right)\cdot\frac{w(d)}{w(d/m^2)}\cdot\frac{|H(d/m^2)/H'|}{|H(d)/H|}.
\end{aligned}$$

Now putting all the above together we get the assertion.

COROLLARY 3.2. *Let d be a discriminant with conductor f. Suppose $n\in\mathbb{N}$ and $(n,f^2)=m^2$ for $m\in\mathbb{N}$. Let H be a subgroup of $H(d)$, $K\in H(d)$, $H_0 = H\cap \operatorname{Ker}\varphi_{1,m}$ and $\operatorname{Ker}\varphi_{1,m}/H_0 = \{A_1H_0,\dots,A_sH_0\}$. Then*

$$R(A_1KH,n) = \cdots = R(A_sKH,n).$$

Proof. Let k and n' be as given in Theorem 3.5. From Corollary 2.2 we see that $\varphi_{k,m}(A_1KH) = \cdots = \varphi_{k,m}(A_sKH)$. Since $\varphi_{k,m}(A_iKH) = \varphi_{k,m}(A_iK)\varphi_{1,m}(H)$ by Theorem 2.5(ii), we see that $\varphi_{k,m}(A_1K)\varphi_{1,m}(H) = \cdots = \varphi_{k,m}(A_sK)\varphi_{1,m}(H)$. Now the result follows immediately from Theorem 3.5.

From Theorem 3.5 and Lemma 2.6 we have

THEOREM 3.6 (Reduction formula for $R(KH^r(d),n)$). *Let d be a discriminant with conductor f and $d_0 = d/f^2$. Let $K\in H(d)$, $n\in\mathbb{N}$ and r be a nonnegative integer. If (n,f^2) is not a square, then $R(KH^r(d),n)=0$. If*

$(n,f^2)=m^2$ *for* $m\in\mathbb{N}$, *and if* k *and* n' *are given as in Theorem* 3.5, *then*

$$\frac{R(KH^r(d),n)}{w(d)}=m\prod_{p\mid m}\Big(1-\frac{1}{p}\Big(\frac{d/m^2}{p}\Big)\Big)\times\frac{|H(d/m^2)/H^r(d/m^2)|}{|H(d)/H^r(d)|}\cdot\frac{R(\varphi_{k,m}(K)H^r(d/m^2),n')}{w(d/m^2)},$$

where p *runs over all distinct prime divisors of* m.

Taking $r=0$ in Theorem 3.6 we obtain

Corollary 3.3 (Reduction formula for $R(K,n)$). *Let* d *be a discriminant with conductor* f *and* $d_0=d/f^2$, *and let* $K\in H(d)$ *and* $n\in\mathbb{N}$. *If* (n,f^2) *is not a square*, *then* $R(K,n)=0$. *If* $(n,f^2)=m^2$ *for* $m\in\mathbb{N}$, *and if* k *and* n' *are given as in Theorem* 3.5, *then*

$$\frac{R(K,n)}{w(d)}=m\prod_{p\mid m}\Big(1-\frac{1}{p}\Big(\frac{d/m^2}{p}\Big)\Big)\cdot\frac{h(d/m^2)}{h(d)}\cdot\frac{R(\varphi_{k,m}(K),n')}{w(d/m^2)},$$

where p *runs over all distinct prime divisors of* m.

For $K\in H(d)$ clearly $R(KH(d),n)=N(n,d)$. Thus putting $r=1$ in Theorem 3.6 we obtain

Corollary 3.4 (Reduction formula for $N(n,d)$). *Let* d *be a discriminant with conductor* f *and* $d_0=d/f^2$. *Let* $n\in\mathbb{N}$. *If* (n,f^2) *is not a square*, *then* $N(n,d)=0$. *If* $(n,f^2)=m^2$ *for* $m\in\mathbb{N}$, *and if* n' *is given by*

$$n'=\prod_{p\nmid d_0}p^{\operatorname{ord}_p(n/m^2)},$$

where p *runs over all distinct prime divisors of* n/m^2, *then*

$$\frac{N(n,d)}{w(d)}=m\prod_{p\mid m}\Big(1-\frac{1}{p}\Big(\frac{d/m^2}{p}\Big)\Big)\cdot\frac{N(n',d/m^2)}{w(d/m^2)},$$

where p *runs over all distinct prime divisors of* m.

Recall that $|G(d)|=|H(d)/H^2(d)|=2^{t(d)}$. Taking $r=2$ in Theorem 3.6 we have

Corollary 3.5 (Reduction formula for $R(G,n)$). *Let* d *be a discriminant with conductor* f *and* $d_0=d/f^2$. *Let* $K\in H(d)$ *and* $n\in\mathbb{N}$. *If* (n,f^2) *is not a square*, *then* $R(KH^2(d),n)=0$. *If* $(n,f^2)=m^2$ *for* $m\in\mathbb{N}$, *and if*

k and n' are as given in Theorem 3.5, *then*

$$\frac{R(KH^2(d),n)}{w(d)} = m\prod_{p\mid m}\left(1-\frac{1}{p}\left(\frac{d/m^2}{p}\right)\right)\cdot\frac{1}{2^{t(d)-t(d/m^2)}} \times \frac{R(\varphi_{k,m}(K)H^2(d/m^2),n')}{w(d/m^2)},$$

where p runs over all distinct prime divisors of m.

REMARK 3.6. Corollary 3.5 unifies and improves the reduction formulas for $R(G,n)$ ($G\in G(d)$) proved in [HKW] and [MW1].

4. Formulas for $N(n,d)$. Let d be a discriminant and $n\in\mathbb{N}$. In this section we give an explicit formula for $N(n,d)$. We also show that $N(n,d)/w(d)$ is a multiplicative function of n and determine the Euler product for the Dirichlet series $\sum_{n=1}^{\infty}\frac{N(n,d)}{w(d)}n^{-s}$ ($\mathrm{Re}(s)>1$).

LEMMA 4.1. *Let d be a discriminant and $n\in\mathbb{N}$. Then $\delta(n,d)=\sum_{m\mid n}\left(\frac{d}{m}\right)$ is a multiplicative function of n and*

$$\delta(n,d) = \begin{cases} \prod_{(\frac{d}{p})=1}(1+\mathrm{ord}_p n) & \text{if } \left(\frac{d}{q}\right)=0,1 \text{ for every prime } q \text{ with } 2\nmid \mathrm{ord}_q n,\\ 0 & \text{otherwise},\end{cases}$$

where in the product p runs over all distinct primes such that $p\mid n$ and $\left(\frac{d}{p}\right)=1$. Moreover, for any complex number s with $\mathrm{Re}(s)>1$ we have

$$\sum_{n=1}^{\infty}\frac{\delta(n,d)}{n^s}=\prod_p\frac{1}{(1-p^{-s})\big(1-\left(\frac{d}{p}\right)p^{-s}\big)},$$

where p runs over all primes.

Proof. Since $\left(\frac{d}{m_1m_2}\right)=\left(\frac{d}{m_1}\right)\left(\frac{d}{m_2}\right)$ for all $m_1,m_2\in\mathbb{N}$ we deduce that $\delta(n,d)$ is a multiplicative function of n. If p is a prime and $t\in\mathbb{N}$, then

$$\delta(p^t,d)=\sum_{m\mid p^t}\left(\frac{d}{m}\right)=\sum_{s=0}^{t}\left(\frac{d}{p^s}\right)=\sum_{s=0}^{t}\left(\frac{d}{p}\right)^s = \begin{cases} t+1 & \text{if } \left(\frac{d}{p}\right)=1,\\ (1+(-1)^t)/2 & \text{if } \left(\frac{d}{p}\right)=-1,\\ 1 & \text{if } p\mid d.\end{cases} \tag{4.1}$$

Write $n=\prod_{p\mid n}p^{\mathrm{ord}_p n}$, where p runs over all distinct prime divisors of n. Then $\delta(n,d)=\prod_{p\mid n}\delta(p^{\mathrm{ord}_p n},d)$. This together with (4.1) gives the formula for $\delta(n,d)$.

Let $d(n)$ denote the number of positive divisors of n. Clearly $0 \le \delta(n,d) \le d(n)$. By [HKW, (9.1)], for any $\varepsilon > 0$ there exists a constant $C(\varepsilon) > 0$ such that $d(n) \le C(\varepsilon)n^{\varepsilon}$. Hence, if $\mathrm{Re}(s) > 1$ and $0 < \varepsilon < \mathrm{Re}(s) - 1$ we have $|\delta(n,d)n^{-s}| \le C(\varepsilon)|n^{-(\mathrm{Re}(s)-\varepsilon)}|$. Thus $\sum_{n=1}^{\infty}\delta(n,d)n^{-s}$ converges absolutely since $\mathrm{Re}(s) - \varepsilon > 1$. Clearly

$$\sum_{n=1}^{\infty}\frac{\delta(n,d)}{n^s} = \Big(\sum_{n=1}^{\infty}\frac{1}{n^s}\Big)\Big(\sum_{n=1}^{\infty}\frac{(\frac{d}{n})}{n^s}\Big) = \prod_p \frac{1}{1-p^{-s}}\prod_p\frac{1}{1-(\frac{d}{p})p^{-s}},$$

where p runs over all primes. This completes the proof.

Let d be a discriminant with conductor f. Let $d_0 = d/f^2$ and $n \in \mathbb{N}$. When $(n,d) = 1$, Dirichlet (cf. [D], [H, pp. 307–308]) proved the following formula for $N(n,d)$:

$$N(n,d) = w(d)\sum_{k\mid n}\Big(\frac{d_0}{k}\Big). \tag{4.2}$$

In 1997 Kaplan and Williams [KW1] showed that this is also true under the weaker condition $(n,f) = 1$. Taking $n = 1$ in (4.2) we find $N(1,d) = w(d)$.

We now give the complete formula for $N(n,d)$. For $d < 0$, the result improves the Huard–Kaplan–Williams formula (see [HKW, Theorem 9.1]).

Theorem 4.1. *Let d be a discriminant with conductor f. Let $d_0 = d/f^2$ and $n \in \mathbb{N}$. If (n,f^2) is not a square, then $N(n,d) = 0$. If $(n,f^2) = m^2$ for $m \in \mathbb{N}$, then*

$$\begin{aligned}\frac{N(n,d)}{w(d)} &= m\prod_{p\mid m}\Big(1-\frac{1}{p}\Big(\frac{d/m^2}{p}\Big)\Big)\cdot\sum_{k\mid \frac{n}{m^2}}\Big(\frac{d_0}{k}\Big)\\ &= \prod_{(\frac{d_0}{p})=-1}\frac{1+(-1)^{\mathrm{ord}_p n}}{2}\cdot m\prod_{p\mid m}\Big(1-\frac{1}{p}\Big(\frac{d/m^2}{p}\Big)\Big)\\ &\quad\times\prod_{(\frac{d_0}{p})=1}\Big(1+\mathrm{ord}_p\frac{n}{m^2}\Big),\end{aligned}$$

where in the products p runs over all distinct primes.

Proof. If (n,f^2) is not a square, by Corollary 3.4 we have $N(n,d) = 0$. We now assume that $(n,f^2) = m^2$ for $m \in \mathbb{N}$. Then $m \mid f$. Let $n' = \prod_{p\nmid d_0} p^{\mathrm{ord}_p(n/m^2)}$, where p runs over all distinct primes such that $p \nmid d_0$ and $p \mid \frac{n}{m^2}$. By Corollary 3.4 we also have

$$\frac{N(n,d)}{w(d)} = m\prod_{p\mid m}\Big(1-\frac{1}{p}\Big(\frac{d/m^2}{p}\Big)\Big)\cdot\frac{N(n',d/m^2)}{w(d/m^2)}.$$

Since $d/m^2 = d_0 f^2/m^2$, $(n', d_0) = 1$ and $(n', f^2/m^2) = 1$ we see that $(n', d/m^2) = 1$. Thus using Dirichlet's formula (4.2) we obtain

$$\frac{N(n', d/m^2)}{w(d/m^2)} = \sum_{k \mid n'} \left(\frac{d_0}{k}\right) = \sum_{k \mid \frac{n}{m^2}} \left(\frac{d_0}{k}\right).$$

Hence combining the above we obtain

$$\frac{N(n,d)}{w(d)} = m \prod_{p \mid m} \left(1 - \frac{1}{p}\left(\frac{d/m^2}{p}\right)\right) \sum_{k \mid \frac{n}{m^2}} \left(\frac{d_0}{k}\right),$$

where p runs over all distinct prime divisors of m. Now applying Lemma 4.1 yields the remaining result. So the theorem is proved.

From Theorem 4.1 and (4.1) we have

COROLLARY 4.1. *Let d be a discriminant with conductor f and $d_0 = d/f^2$. Let p be a prime and let t be a nonnegative integer.*

(i) *If $p \nmid f$, then*

$$N(p^t, d) = \begin{cases} 0 & \text{if } 2 \nmid t \text{ and } \left(\frac{d_0}{p}\right) = -1, \\ w(d)(t+1) & \text{if } \left(\frac{d_0}{p}\right) = 1, \\ w(d) & \text{otherwise.} \end{cases}$$

(ii) *If $p \mid f$, say that $p^\alpha \parallel f$, then*

$$N(p^t, d) = \begin{cases} 0 & \text{if } 2 \nmid t \text{ and } \left(\frac{d_0}{p}\right) = -1, \\ 0 & \text{if } 2 \nmid t,\ t < 2\alpha \text{ and } \left(\frac{d_0}{p}\right) = 0, 1, \\ w(d) p^{t/2} & \text{if } 2 \mid t \text{ and } t < 2\alpha, \\ w(d)(p^\alpha - p^{\alpha-1})(t + 1 - 2\alpha) & \text{if } t \ge 2\alpha \text{ and } \left(\frac{d_0}{p}\right) = 1, \\ w(d) p^\alpha & \text{if } t \ge 2\alpha \text{ and } p \mid d_0, \\ w(d)(p^\alpha + p^{\alpha-1}) & \text{if } t \ge 2\alpha,\ 2 \mid t \text{ and } \left(\frac{d_0}{p}\right) = -1. \end{cases}$$

The following result follows immediately from Corollary 4.1.

COROLLARY 4.2. *Let d be a discriminant with conductor f and $d_0 = d/f^2$. Let p be a prime and let t be a nonnegative integer. Then p^t is represented by at least one class in $H(d)$ if and only if $2 \mid t$ or $\left(\frac{d_0}{p}\right) = 0, 1$ and $p^t \nmid f^2$.*

THEOREM 4.2. *Let d be a discriminant. Then $N(n,d)/w(d)$ is a multiplicative function of $n \in \mathbb{N}$.*

Proof. Let f be the conductor of d and $d_0 = d/f^2$. Suppose that n_1 and n_2 are relatively prime positive integers. Then clearly $(n_1 n_2, f^2) =$

$(n_1, f^2)(n_2, f^2)$. Thus, if $(n_1 n_2, f^2)$ is not a square, then either (n_1, f^2) or (n_2, f^2) is not a square. Hence by Theorem 4.1 we have

$$\frac{N(n_1 n_2, d)}{w(d)} = 0 = \frac{N(n_1, d)}{w(d)} \cdot \frac{N(n_2, d)}{w(d)}.$$

Now suppose that $(n_1 n_2, f^2)$ is a square. Since $(n_1, n_2) = 1$ and so $(n_1 n_2, f^2) = (n_1, f^2)(n_2, f^2)$ we see that $(n_1, f^2) = m_1^2$ and $(n_2, f^2) = m_2^2$ for some $m_1, m_2 \in \mathbb{N}$ and $(m_1, m_2) = 1$. By Theorem 4.1 and Lemma 4.1 we have

$$\begin{aligned}\frac{N(n_1 n_2, d)}{w(d)} &= m_1 m_2 \prod_{p \mid m_1 m_2} \left(1 - \frac{1}{p}\left(\frac{d/(m_1^2 m_2^2)}{p}\right)\right) \delta\left(\frac{n_1 n_2}{m_1^2 m_2^2}, d_0\right) \\ &= \prod_{i=1}^{2} m_i \prod_{p \mid m_i} \left(1 - \frac{1}{p}\left(\frac{d/m_i^2}{p}\right)\right) \delta\left(\frac{n_i}{m_i^2}, d_0\right) \\ &= \frac{N(n_1, d)}{w(d)} \cdot \frac{N(n_2, d)}{w(d)},\end{aligned}$$

where in the products p runs over all distinct primes. This finishes the proof.

From Theorem 4.2 we have

Corollary 4.3. *Let d be a discriminant such that $h(d) = 1$. Let $\delta_d = 0$ or 1 according as $2 \mid d$ or $2 \nmid d$. Then $R([1, \delta_d, (-d + \delta_d)/4], n)/w(d)$ is a multiplicative function of $n \in \mathbb{N}$.*

Remark 4.1. When $h(d) = 1$, $R([1, \delta_d, (-d + \delta_d)/4], n) = N(n, d)$ is given by Theorem 4.1. The values of $d < 0$ for which $h(d) = 1$ are known, see for example [Cox, p. 149]. We have $h(d) = 1 \Leftrightarrow d = -3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163$. For $d > 0$, we know that $h(d) = 1$ for $d = 5, 8, 13, 17, 20, 29, 37, 41, 52, 53, 61, 68, 73, 89, 97, \ldots$.

Theorem 4.3. *Let d be a discriminant with conductor f and $d_0 = d/f^2$. Let s be a complex number with $\mathrm{Re}(s) > 1$. Then the Dirichlet series $\sum_{n=1}^{\infty} \frac{N(n,d)/w(d)}{n^s}$ converges absolutely and*

$$\begin{aligned}\sum_{n=1}^{\infty} \frac{N(n, d)/w(d)}{n^s} = \prod_{p \mid f} &\left(\frac{1 - p^{\alpha_p(1-2s)}}{1 - p^{1-2s}} + \frac{p^{\alpha_p(1-2s)}\left(1 - \frac{1}{p}\left(\frac{d_0}{p}\right)\right)}{(1 - p^{-s})\left(1 - \left(\frac{d_0}{p}\right)p^{-s}\right)}\right) \\ &\times \prod_{p \nmid f} \frac{1}{(1 - p^{-s})\left(1 - \left(\frac{d_0}{p}\right)p^{-s}\right)},\end{aligned}$$

where p runs over all primes and $\alpha_p = \mathrm{ord}_p f$.

Proof. From Theorem 4.2 we know that $N(n,d)/w(d)$ is a multiplicative function of $n\in\mathbb{N}$. By Theorem 4.1 and the same argument as in the proof of [HKW, Corollary 9.1], for any $\varepsilon>0$ there exists a constant $C(\varepsilon)$ such that $N(n,d)\le C(\varepsilon)n^{\varepsilon}$. Letting $\varepsilon\in(0,\mathrm{Re}(s)-1)$ we see that $\sum_{n=1}^{\infty}\frac{N(n,d)}{w(d)}n^{-s}$ converges absolutely. Thus

$$\sum_{n=1}^{\infty}\frac{N(n,d)/w(d)}{n^s}=\prod_{p\mid f}\Big(1+\sum_{t=1}^{\infty}\frac{N(p^t,d)}{w(d)}\,p^{-st}\Big)\prod_{p\nmid f}\Big(1+\sum_{t=1}^{\infty}\frac{N(p^t,d)}{w(d)}\,p^{-st}\Big).$$

From Theorem 4.2, (4.2) and Lemma 4.1 we have

$$\begin{aligned}\prod_{p\nmid f}\Big(1+\sum_{t=1}^{\infty}\frac{N(p^t,d)}{w(d)}\,p^{-st}\Big)&=\sum_{\substack{n=1\\(n,f)=1}}^{\infty}\frac{N(n,d)/w(d)}{n^s}=\sum_{\substack{n=1\\(n,f)=1}}^{\infty}\frac{\delta(n,d_0)}{n^s}\\&=\prod_{p\nmid f}\frac{1}{(1-p^{-s})\big(1-\big(\frac{d_0}{p}\big)p^{-s}\big)},\end{aligned}$$

where p runs over all primes not dividing f.

If p is a prime such that $p\mid f$, letting $p^{\alpha_p}\parallel f$ and using Corollary 4.1 we see that

$$\begin{aligned}1+&\sum_{1\le t<2\alpha_p}\frac{N(p^t,d)}{w(d)}\,p^{-st}\\&=\sum_{\substack{0\le t<2\alpha_p\\2\mid t}}p^{t/2}\cdot p^{-st}=\sum_{0\le r<\alpha_p}p^{r(1-2s)}=\frac{1-p^{\alpha_p(1-2s)}}{1-p^{1-2s}}\end{aligned}$$

and

$$\sum_{t\ge 2\alpha_p}\frac{N(p^t,d)}{w(d)}\,p^{-st}$$

$$=\begin{cases}\displaystyle\sum_{t\ge2\alpha_p}p^{\alpha_p}\cdot p^{-st}=\frac{p^{\alpha_p(1-2s)}}{1-p^{-s}} & \text{if } p\mid d_0,\\ \displaystyle\sum_{\substack{t\ge2\alpha_p\\2\mid t}}(p^{\alpha_p}+p^{\alpha_p-1})p^{-st}=(p^{\alpha_p}+p^{\alpha_p-1})\frac{p^{-2s\alpha_p}}{1-p^{-2s}} & \text{if } \big(\frac{d_0}{p}\big)=-1,\\ \displaystyle\sum_{t\ge2\alpha_p}(p^{\alpha_p}-p^{\alpha_p-1})(t+1-2\alpha_p)p^{-st}=(p^{\alpha_p}-p^{\alpha_p-1})\frac{p^{-2s\alpha_p}}{(1-p^{-s})^2} & \\ & \text{if } \big(\frac{d_0}{p}\big)=1.\end{cases}$$

In the last case we use the fact that

$$\begin{aligned}\sum_{t=0}^{\infty}(t+1)x^t&=\frac{d}{dx}\Big(\sum_{t=0}^{\infty}x^{t+1}\Big)=\frac{d}{dx}\Big(\frac{x}{1-x}\Big)\\&=\frac{1}{(1-x)^2}\qquad(|x|<1).\end{aligned}\tag{4.3}$$

From the above we obtain

$$\prod_{p\mid f}\Big(1+\sum_{t=1}^{\infty}\frac{N(p^t,d)}{w(d)}\,p^{-st}\Big)$$
$$=\prod_{p\mid f}\Big(1+\sum_{1\le t<2\alpha_p}\frac{N(p^t,d)}{w(d)}\,p^{-st}+\sum_{t\ge 2\alpha_p}\frac{N(p^t,d)}{w(d)}\,p^{-st}\Big)$$
$$=\prod_{p\mid f}\Big(\frac{1-p^{\alpha_p(1-2s)}}{1-p^{1-2s}}+\frac{p^{\alpha_p(1-2s)}\big(1-\frac{1}{p}\big(\frac{d_0}{p}\big)\big)}{(1-p^{-s})\big(1-\big(\frac{d_0}{p}\big)p^{-s}\big)}\Big),$$

where p runs over all distinct prime divisors of f.

Now putting all the above together we get the assertion.

From Remark 4.1 and Theorem 4.3 we deduce

Corollary 4.4. *For $k\in\mathbb{Z}$ let $\delta_k=0$ or 1 according as $2\mid k$ or $2\nmid k$. Let s be a complex number with* $\mathrm{Re}(s)>1$.

(i) *Let $d\in\{-3,-4,-7,-8,-11,-19,-43,-67,-163\}$. Then*

$$\sum_{n=1}^{\infty}\frac{R([1,\delta_d,(-d+\delta_d)/4],n)/w(d)}{n^s}=\prod_p\frac{1}{(1-p^{-s})\big(1-\big(\frac{d}{p}\big)p^{-s}\big)},$$

where p runs over all primes.

(ii) *We have*

$$\sum_{n=1}^{\infty}\frac{\frac12 R([1,0,3],n)}{n^s}=\frac{1+2^{1-2s}}{1-2^{-2s}}\cdot\frac{1}{1-3^{-s}}\prod_{p\equiv 1\,(\mathrm{mod}\,6)}\frac{1}{(1-p^{-s})^2}\prod_{p\equiv 5\,(\mathrm{mod}\,6)}\frac{1}{1-p^{-2s}},$$

$$\sum_{n=1}^{\infty}\frac{\frac12 R([1,0,4],n)}{n^s}=\frac{1-2^{-s}+2^{1-2s}}{1-2^{-s}}\prod_{p\equiv 1\,(\mathrm{mod}\,4)}\frac{1}{(1-p^{-s})^2}\prod_{p\equiv 3\,(\mathrm{mod}\,4)}\frac{1}{1-p^{-2s}},$$

$$\sum_{n=1}^{\infty}\frac{\frac12 R([1,1,7],n)}{n^s}=\frac{1-3^{-s}+3^{1-2s}}{1-3^{-s}}\prod_{p\equiv 1\,(\mathrm{mod}\,3)}\frac{1}{(1-p^{-s})^2}\prod_{p\equiv 2\,(\mathrm{mod}\,3)}\frac{1}{1-p^{-2s}}$$

and

$$\sum_{n=1}^{\infty}\frac{\frac12 R([1,0,7],n)}{n^s} = \frac{1-2^{1-s}+2^{1-2s}}{(1-2^{-s})^2}\cdot\frac{1}{1-7^{-s}}\prod_{p\equiv 1,9,11\ (\mathrm{mod}\ 14)}\frac{1}{(1-p^{-s})^2} \times\prod_{p\equiv 3,5,13\ (\mathrm{mod}\ 14)}\frac{1}{1-p^{-2s}},$$

where p runs over all primes.

5. Formulas for $R(K,p^t)$ and $R'(K,p^t)$. Let d be a discriminant and $K\in H(d)$. In the section we completely determine $R(K,p^t)$ and $R'(K,p^t)$, where p is a prime and t is a nonnegative integer.

For $n\in\mathbb{N}$ let $H_{[a,b,c]}(n)$ and $R'([a,b,c],n)$ be defined by Definitions 3.1 and 3.2 respectively. From Theorem 3.1 we have

Lemma 5.1. *Let d be a discriminant and $a,b,c\in\mathbb{Z}$ with $b^2-4ac=d$. Suppose that p is a prime and t is a nonnegative integer. Then*

$$R([a,b,c],p^t)=\sum_{r=0}^{[t/2]}R'([a,b,c],p^{t-2r})=w(d)\sum_{r=0}^{[t/2]}H_{[a,b,c]}(p^{t-2r})$$

and

$$R'([a,b,c],p^t)=w(d)H_{[a,b,c]}(p^t) =\begin{cases}R([a,b,c],p^t) & \text{if } t=0,1,\\ R([a,b,c],p^t)-R([a,b,c],p^{t-2}) & \text{if } t\ge 2.\end{cases}$$

In [MW2], Muzaffar and Williams discussed $H_K(n)$ $(K\in H(d))$ for $d<0$. After checking their proofs, we note that Lemmas 5.1–5.5 of [MW2] are also true for $d>0$. Thus it follows from [MW2, Lemma 5.2] that $H_K(1)=1$ or 0 according as K is the principal class I or not. Hence by Lemma 5.1 we have

$$(5.1)\qquad R(K,1)=R'(K,1)=w(d)H_K(1)=\begin{cases}w(d) & \text{if } K=I,\\ 0 & \text{if } K\ne I.\end{cases}$$

Let p be a prime. Let f be the conductor of d. Clearly $H_K(p)\in\{0,1,2\}$ by Definition 3.1. By Corollary 4.2, p is represented by some class in $H(d)$ if and only if $\left(\frac{d}{p}\right)=0,1$ and $p\nmid f$. If p is represented by the class A in $H(d)$, then p is also represented by A^{-1} since $R(A,p)=R(A^{-1},p)$. By Lemma 5.1 we have $R(K,p)=R'(K,p)=w(d)H_K(p)$. From this and [MW2, Lemma 5.3] we deduce

Lemma 5.2. *Let d be a discriminant with conductor f. Let p be a prime and $K\in H(d)$.*

(i) *p is represented by some class in $H(d)$ if and only if $\left(\frac{d}{p}\right)=0,1$ and $p\nmid f$.*

(ii) *Suppose $p\,|\,d$ and $p\nmid f$. Then p is represented by exactly one class $A\in H(d)$, and $A=A^{-1}$. Moreover, $R(A,p)=R'(A,p)=w(d)$. Thus, if $h(d)$ is odd, then $R(I,p)=R'(I,p)=w(d)$ and $R(K,p)=R'(K,p)=0$ for $K\neq I$.*

(iii) *Suppose $\left(\frac{d}{p}\right)=1$. Then p is represented by some class $A\in H(d)$, and*

$$R(K,p)=R'(K,p)=\begin{cases}0 & \text{if } K\neq A,A^{-1},\\ w(d) & \text{if } A\neq A^{-1} \text{ and } K\in\{A,A^{-1}\},\\ 2w(d) & \text{if } K=A=A^{-1}.\end{cases}$$

Let t be a nonnegative integer and $K\in H(d)$. From now on we set

$$\delta_K(t)=\begin{cases}1 & \text{if } 2\,|\,t \text{ and } K=I,\\ 0 & \text{otherwise.}\end{cases}\tag{5.2}$$

From (5.1) and Lemma 5.1 we find that if p is a prime, then

$$R(K,p^t)=w(d)\Big(\delta_K(t)+\sum_{0\le r<t/2}H_K(p^{t-2r})\Big).\tag{5.3}$$

From [MW2, Lemma 5.4] we also know that if p is a prime and $s\in\{2,3,\dots\}$, then

$$H_K(p^s)=\begin{cases}\displaystyle\sum_{\substack{L\in H(d)\\ L^s=K}}H_L(p) & \text{if } p\nmid d,\\ 0 & \text{if } p\,|\,d \text{ and } p\nmid f.\end{cases}\tag{5.4}$$

We now determine $R(K,p^t)$ when $p\nmid f$.

Theorem 5.1. *Let d be a discriminant with conductor f, and let p be a prime such that $p\nmid f$. Let t be a nonnegative integer and $K\in H(d)$.*

(i) *If $\left(\frac{d}{p}\right)=-1$, then*

$$R(K,p^t)=\begin{cases}w(d) & \text{if } 2\,|\,t \text{ and } K=I,\\ 0 & \text{otherwise.}\end{cases}$$

(ii) *If $p\,|\,d$, then*

$$R(K,p^t)=\begin{cases}w(d) & \text{if } 2\,|\,t \text{ and } K=I, \text{ or if } 2\nmid t \text{ and } p \text{ is represented by } K,\\ 0 & \text{otherwise.}\end{cases}$$

(iii) *Suppose $\left(\frac{d}{p}\right)=1$ so that p is only represented by some class A and the inverse A^{-1} in $H(d)$. Let m be the order of A in $H(d)$. If K*

is not a power of A, then $R(K,p^t)=0$. If $k,t_0\in\{0,1,\ldots,m-1\}$ with $t_0\equiv t \pmod m$, then

$$R(A^k,p^t)=\begin{cases}0 & \text{if } 2\mid m \text{ and } 2\nmid k-t,\\ w(d)\Big(\Big[\frac{t}{m/(2,m)}\Big]+1\Big) & \text{if } t_0\in S_{k,m},\\ w(d)\Big[\frac{t}{m/(2,m)}\Big] & \text{otherwise,}\end{cases}$$

where

$$S_{k,m}=\begin{cases}\{r\mid k\le r<m,\ 2\mid k-r\}\cup\{r\mid m-k\le r<m,\ 2\nmid k-r\} & \text{if } 2\nmid m,\\ \{r\mid \min\{k,m-k\}\le r<m/2,\ 2\mid k-r\}\\ \quad\cup\{r\mid \max\{k,m-k\}\le r<m,\ 2\mid k-r\} & \text{if } 2\mid m.\end{cases}$$

Proof. Let $\delta_K(t)$ be given by (5.2). We first assume $\left(\frac{d}{p}\right)=-1$. If $t=0$, the result follows from (5.1). If $t\ge 1$, then the congruence $x^2\equiv d \pmod{4p^t}$ is insolvable. Hence $H_K(p^t)=0$ for every $K\in H(d)$. Using (5.3) we see that $R(K,p^t)=w(d)\delta_K(t)$. This proves (i).

Next we consider (ii). If $t=0$, the result follows from (5.1). For $t=1$ the result follows from Lemma 5.2(ii). When $t\ge 2$, by [MW2, Lemma 5.4] we have $H_K(p^t)=0$. Hence applying (5.3) and Lemma 5.2(ii) we obtain the result.

Finally we consider (iii). By [MW2, Lemma 5.3], $H_L(p)=0$ for $L\ne A,A^{-1}$ and $H_A(p)=2$ or 1 according as $A=A^{-1}$ or not. Thus applying (5.3) and (5.4) we deduce

$$\begin{aligned}\frac{R(K,p^t)}{w(d)}&=\delta_K(t)+\sum_{0\le r<t/2}\ \sum_{\substack{L\in H(d)\\ L^{t-2r}=K}}H_L(p)\\ &=\delta_K(t)+\sum_{L\in H(d)}H_L(p)\sum_{\substack{0\le r<t/2\\ L^{t-2r}=K}}1\\ &=\delta_K(t)+\sum_{\substack{0\le r<t/2\\ A^{t-2r}=K}}1+\sum_{\substack{0\le r<t/2\\ A^{-(t-2r)}=K}}1\\ &=\sum_{\substack{0\le r\le t/2\\ A^{t-2r}=K}}1+\sum_{\substack{0\le r<t/2\\ A^{-(t-2r)}=K}}1.\end{aligned}$$

Hence, if K is not a power of A, then $R(K,p^t)=0$. Now assume $k\in\{0,1,\ldots,m-1\}$. From the above we have

$$(5.5)\qquad \frac{R(A^k,p^t)}{w(d)} = \sum_{\substack{0\le r\le t/2\\ t-2r\equiv k \pmod m}} 1 + \sum_{\substack{0\le r< t/2\\ t-2r\equiv -k \pmod m}} 1$$

$$= \begin{cases} 0 & \text{if } (2,m)\nmid k-t,\\ \displaystyle\sum_{\substack{0\le r\le t/2\\ r\equiv \frac{t-k}{2} \ (\mathrm{mod}\ \frac{m}{(2,m)})}} 1 + \sum_{\substack{0\le r< t/2\\ r\equiv \frac{t+k}{2} \ (\mathrm{mod}\ \frac{m}{(2,m)})}} 1 & \text{if } (2,m)\mid k-t. \end{cases}$$

If $a,n\in\mathbb{N}$, $a-n\le t/2<a$ and $a=n\left[\frac{a}{n}\right]+a_0$, then $a_0\in\{0,1,\dots,n-1\}$ and therefore

$$\sum_{\substack{0\le r\le t/2\\ r\equiv a \pmod n}} 1 = |\{s\in\mathbb{Z}\mid 0\le a_0+sn\le t/2\}|$$
$$= |\{s\mid s\in\{0,1,\dots,[a/n]-1\}| = \left[\frac{a}{n}\right].$$

Using this we see that

$$\sum_{\substack{0\le r\le t/2\\ r\equiv \frac{t-k}{2} \ (\mathrm{mod}\ \frac{m}{(2,m)})}} 1 = \begin{cases} \displaystyle\sum_{\substack{0\le r\le t/2\\ r\equiv \frac{t+m-k}{2} \ (\mathrm{mod}\ \frac{m}{2})}} 1 = \left[\frac{(t+m-k)/2}{m/2}\right] = \left[\frac{t+m-k}{m}\right] & \text{if } 2\mid m \text{ and } 2\mid k-t,\\ \displaystyle\sum_{\substack{0\le r\le t/2\\ r\equiv \frac{t+2m-k}{2} \pmod m}} 1 = \left[\frac{(t+2m-k)/2}{m}\right] = \left[\frac{t+2m-k}{2m}\right] & \text{if } 2\nmid m \text{ and } 2\mid k-t,\\ \displaystyle\sum_{\substack{0\le r\le t/2\\ r\equiv \frac{t+m-k}{2} \pmod m}} 1 = \left[\frac{(t+m-k)/2}{m}\right] = \left[\frac{t+m-k}{2m}\right] & \text{if } 2\nmid m(k-t). \end{cases}$$

Similarly, if $a,n\in\mathbb{N}$ are such that $a-n<t/2\le a$ then

$$\sum_{\substack{0\le r<t/2\\ r\equiv a \pmod n}} 1 = \left[\frac{a}{n}\right].$$

Using this we obtain

$$\sum_{\substack{0\le r< t/2\\ r\equiv \frac{t+k}{2} \ (\mathrm{mod}\ \frac{m}{(2,m)})}} 1 = \begin{cases} \left[\frac{(t+k)/2}{m/2}\right] = \left[\frac{t+k}{m}\right] & \text{if } 2\mid m \text{ and } 2\mid k-t,\\ \left[\frac{(t+k)/2}{m}\right] = \left[\frac{t+k}{2m}\right] & \text{if } 2\nmid m \text{ and } 2\mid k-t,\\ \left[\frac{(t+m+k)/2}{m}\right] = \left[\frac{t+m+k}{2m}\right] & \text{if } 2\nmid m(k-t). \end{cases}$$

Hence

$$(5.6) \qquad \frac{R(A^k, p^t)}{w(d)} = \begin{cases} 0 & \text{if } 2 \mid m \text{ and } 2 \nmid k - t, \\ \left[\frac{t+m-k}{m}\right] + \left[\frac{t+k}{m}\right] & \text{if } 2 \mid m \text{ and } 2 \mid k-t, \\ \left[\frac{t+2m-k}{2m}\right] + \left[\frac{t+k}{2m}\right] & \text{if } 2 \nmid m \text{ and } 2 \mid k-t, \\ \left[\frac{t+m-k}{2m}\right] + \left[\frac{t+m+k}{2m}\right] & \text{if } 2 \nmid m \text{ and } 2 \nmid k-t. \end{cases}$$

Set $s = [t/m]$. Then $t = sm + t_0$. We first assume $2 \nmid m$. Clearly $k - t = k - sm - t_0 \equiv k - t_0 - s \pmod 2$. Thus $2 \mid k - t_0$ if and only if $k - t \equiv s \pmod 2$. If $2 \mid k - t_0$, by (5.6) we have

$$\begin{aligned} \frac{R(A^k, p^t)}{w(d)} &= \begin{cases} \left[\frac{t+2m-k}{2m}\right] + \left[\frac{t+k}{2m}\right] & \text{if } 2 \mid s \text{ and } 2 \mid k-t, \\ \left[\frac{t+m-k}{2m}\right] + \left[\frac{t+m+k}{2m}\right] & \text{if } 2 \nmid s \text{ and } 2 \nmid k-t \end{cases} \\ &= s + 1 + \left[\frac{t_0-k}{2m}\right] + \left[\frac{t_0+k}{2m}\right] = s + 1 + \left[\frac{t_0-k}{2m}\right] \\ &= \begin{cases} s+1 & \text{if } t_0 \ge k, \\ s & \text{if } t_0 < k. \end{cases} \end{aligned}$$

If $2 \nmid k - t_0$, by (5.6) we get

$$\begin{aligned} \frac{R(A^k, p^t)}{w(d)} &= \begin{cases} \left[\frac{t+2m-k}{2m}\right] + \left[\frac{t+k}{2m}\right] & \text{if } 2 \nmid s \text{ and } 2 \mid k-t, \\ \left[\frac{t+m-k}{2m}\right] + \left[\frac{t+m+k}{2m}\right] & \text{if } 2 \mid s \text{ and } 2 \nmid k-t \end{cases} \\ &= s + \left[\frac{m+t_0-k}{2m}\right] + \left[\frac{m+t_0+k}{2m}\right] = s + \left[\frac{m+t_0+k}{2m}\right] \\ &= \begin{cases} s+1 & \text{if } t_0 + k \ge m, \\ s & \text{if } t_0 + k < m. \end{cases} \end{aligned}$$

Thus $R(A^k, p^t) = (s+1)w(d)$ or $sw(d)$ according as $t_0 \in S_{k,m}$ or not.

Now suppose $2 \mid m$ and $2 \mid k - t$. So $2 \mid k - t_0$. By (5.6) we obtain

$$\begin{aligned} \frac{R(A^k, p^t)}{w(d)} &= \left[\frac{t+m-k}{m}\right] + \left[\frac{t+k}{m}\right] \\ &= \left[\frac{sm+m+t_0-k}{m}\right] + \left[\frac{sm+t_0+k}{m}\right] \end{aligned}$$

$$= 2s + 1 + \left[\frac{t_0 - k}{m}\right] + \left[\frac{t_0 + k}{m}\right]$$

$$= \begin{cases} 2s+2 & \text{if } t_0 \ge \max\{k, m-k\}, \\ 2s+1 & \text{if } \min\{k, m-k\} \le t_0 < \max\{k, m-k\}, \\ 2s & \text{if } t_0 < \min\{k, m-k\}. \end{cases}$$

Note that

$$\left[\frac{t}{m/2}\right] = \left[\frac{sm + t_0}{m/2}\right] = 2s + \left[\frac{t_0}{m/2}\right] = \begin{cases} 2s+1 & \text{if } t_0 \ge m/2, \\ 2s & \text{if } t_0 < m/2. \end{cases}$$

Applying the above we see that

$$\frac{R(A^k, p^t)}{w(d)} = \begin{cases} 2s+2 = \left[\frac{t}{m/2}\right] + 1 & \text{if } t_0 \ge \max\{k, m-k\}, \\ 2s+1 = \left[\frac{t}{m/2}\right] + 1 & \text{if } \min\{k, m-k\} \le t_0 < m/2, \\ 2s+1 = \left[\frac{t}{m/2}\right] & \text{if } m/2 \le t_0 < \max\{k, m-k\}, \\ 2s = \left[\frac{t}{m/2}\right] & \text{if } t_0 < \min\{k, m-k\}. \end{cases}$$

Therefore, $R(A^k, p^t)/w(d) = \left[\frac{t}{m/2}\right] + 1$ or $\left[\frac{t}{m/2}\right]$ according as $t_0 \in S_{k,m}$ or $t_0 \notin S_{k,m}$. So (iii) is true and hence the theorem is proved.

THEOREM 5.2. *Let d be a discriminant with conductor f, and let p be a prime such that $p \nmid f$. Let $t \in \mathbb{N}$, $t \ge 2$ and $K \in H(d)$.*

(i) *If $\left(\frac{d}{p}\right) = 0, -1$, then $R'(K, p^t) = 0$.*

(ii) *Suppose $\left(\frac{d}{p}\right) = 1$ so that p is represented by some $A \in H(d)$. Let m be the order of A in $H(d)$. If K is not a power of A, then $R'(K, p^t) = 0$. If $k \in \mathbb{Z}$, then*

$$R'(A^k, p^t) = \begin{cases} 0 & \textit{if } t \not\equiv \pm k \pmod m, \\ w(d) & \textit{if } t \equiv \pm k \pmod m \textit{ and } m \nmid 2k, \\ 2w(d) & \textit{if } t \equiv k \equiv -k \pmod m. \end{cases}$$

Proof. As $t \ge 2$, by Lemma 5.1 we have $R'(K, p^t) = R(K, p^t) - R(K, p^{t-2})$. Thus (i) follows from Theorem 5.1. Now we consider (ii). From the above and (5.5) we see that

$$
\begin{aligned}
\frac{R'(A^k,p^t)}{w(d)} &= \frac{R(A^k,p^t)}{w(d)} - \frac{R(A^k,p^{t-2})}{w(d)} \\
&= \sum_{\substack{0\le r\le t/2\\ t-2r\equiv k \,(\mathrm{mod}\, m)}} 1 + \sum_{\substack{0\le r< t/2\\ t-2r\equiv -k \,(\mathrm{mod}\, m)}} 1 \\
&\quad - \sum_{\substack{0\le s\le (t-2)/2\\ t-2-2s\equiv k \,(\mathrm{mod}\, m)}} 1 - \sum_{\substack{0\le s< (t-2)/2\\ t-2-2s\equiv -k \,(\mathrm{mod}\, m)}} 1 \\
&= \sum_{\substack{0\le r\le t/2\\ t-2r\equiv k \,(\mathrm{mod}\, m)}} 1 + \sum_{\substack{0\le r< t/2\\ t-2r\equiv -k \,(\mathrm{mod}\, m)}} 1 \\
&\quad - \sum_{\substack{1\le r\le t/2\\ t-2r\equiv k \,(\mathrm{mod}\, m)}} 1 - \sum_{\substack{1\le r< t/2\\ t-2r\equiv -k \,(\mathrm{mod}\, m)}} 1 \\
&= \chi(m\,|\,t-k) + \chi(m\,|\,t+k),
\end{aligned}
$$

where $\chi(a\,|\,b) = 1$ or 0 according as $a\,|\,b$ or not. This yields (ii) and hence the theorem is proved.

THEOREM 5.3. *Let d be a discriminant with conductor f and $d_0 = d/f^2$. Let p be a prime dividing f and $p^\alpha \,\|\, f$. Let $K \in H(d)$, $t \in \mathbb{N}$ and $K_p = \varphi_{1,p^\alpha}(K) \in H(d/p^{2\alpha})$. In view of Lemma 3.5, for $s \in \{1,\dots,\alpha\}$ set*

$$
W_{p^s} = p^{s-1}\left(p - \left(\frac{d/p^{2s}}{p}\right)\right)\frac{h(d/p^{2s})w(d)}{h(d)} = \begin{cases} w(d/p^{2s}) & \text{if } d<0,\\ \dfrac{\log\varepsilon(d)}{\log\varepsilon(d/p^{2s})} & \text{if } d>0.\end{cases}
$$

(i) *If $t \le 2\alpha$, then*

$$
R(K,p^t) = \begin{cases} W_{p^{t/2}} & \text{if } 2\,|\,t \text{ and } \varphi_{1,p^{t/2}}(K) \text{ is the principal class in } H(d/p^t),\\ 0 & \text{otherwise.}\end{cases}
$$

(ii) *If $t \ge 2\alpha$, then*

$$
R(K,p^t) = \begin{cases} R(K_p,p^{t-2\alpha}) & \text{if } d<0,\\ W_{p^\alpha} R(K_p,p^{t-2\alpha}) & \text{if } d>0.\end{cases}
$$

(iii) *If $t > 2\alpha$ and $\left(\frac{d_0}{p}\right) = -1$, then*

$$
R(K,p^t) = \begin{cases} W_{p^\alpha} & \text{if } 2\,|\,t \text{ and } K_p \text{ is the principal class in } H(d/p^{2\alpha}),\\ 0 & \text{otherwise.}\end{cases}
$$

(iv) *If $t > 2\alpha$ and $p\,|\,d_0$, then*

$$
R(K,p^t) = \begin{cases} W_{p^\alpha} & \text{if } 2\nmid t \text{ and } p \text{ is represented by } K_p, \text{ or if } 2\,|\,t \\ & \qquad \text{and } K_p \text{ is the principal class in } H(d/p^{2\alpha}),\\ 0 & \text{otherwise.}\end{cases}
$$

(v) *Suppose* $t > 2\alpha$, $\left(\frac{d_0}{p}\right) = 1$ *and* p *is represented by the class* $A \in H(d/p^{2\alpha})$ *of order* m. *If* K_p *is not a power of* A, *then* $R(K, p^t) = 0$. *If* $k, t_0 \in \{0, 1, \dots, m-1\}$ *with* $K_p = A^k$ *and* $t_0 \equiv t - 2\alpha \pmod m$, *then*

$$R(K,p^t) = \begin{cases} 0 & \text{if } 2\,|\,m \text{ and } 2\nmid k-t, \\ W_{p^\alpha}\left(\left[\dfrac{t-2\alpha}{m/(2,m)}\right]+1\right) & \text{if } t_0 \in S_{k,m}, \\ W_{p^\alpha}\left[\dfrac{t-2\alpha}{m/(2,m)}\right] & \text{otherwise,} \end{cases}$$

where the set $S_{k,m}$ *is defined as in Theorem* 5.1.

Proof. Clearly $(p^t, f^2) = (p^t, p^{2\alpha}) = p^{\min\{t,2\alpha\}}$. If $t \le 2\alpha$, then $(p^t, f^2) = p^t$. Thus using Theorem 3.2 we see that

$$R(K,p^t) = \begin{cases} 0 & \text{if } 2\nmid t, \\ R(\varphi_{1,p^{t/2}}(K), 1) & \text{if } 2\,|\,t \text{ and } d<0, \\ \dfrac{\log\varepsilon(d)}{\log\varepsilon(d/p^t)}\,R(\varphi_{1,p^{t/2}}(K), 1) & \text{if } 2\,|\,t \text{ and } d>0. \end{cases}$$

Now applying (5.1) we obtain (i).

If $t \ge 2\alpha$, then $(p^t, f^2) = p^{2\alpha}$. Applying Theorem 3.2 we see that (ii) is true.

Since $K_p \in H(d/p^{2\alpha})$, $d/p^{2\alpha} = d_0(f/p^\alpha)^2$ and $(p^{t-2\alpha}, f/p^\alpha) = 1$, by (ii) and Theorem 5.1 we obtain (iii), (iv) and (v).

Theorem 5.4. *Suppose all the assumptions in Theorem* 5.3 *hold.*

(i) *For* $t \le 2\alpha$ *we have*

$$R'(K,p^t) = \begin{cases} W_{p^{t/2}} & \text{if } 2\,|\,t \text{ and } K \in \operatorname{Ker}\varphi_{1,p^{t/2}} - \operatorname{Ker}\varphi_{1,p^{t/2-1}}, \\ W_{p^{t/2}} - W_{p^{t/2-1}} & \text{if } 2\,|\,t \text{ and } K \in \operatorname{Ker}\varphi_{1,p^{t/2-1}}, \\ 0 & \text{otherwise.} \end{cases}$$

(ii) *For* $t = 2\alpha + 1$ *we have*

$$R'(K,p^{2\alpha+1}) = \begin{cases} W_{p^\alpha} & \text{if } \left(\frac{d_0}{p}\right)=1,\ p \text{ is represented by } K_p \text{ and } K_p \ne K_p^{-1}, \\ & \quad \text{or if } p\,|\,d_0 \text{ and } p \text{ is represented by } K_p, \\ 2W_{p^\alpha} & \text{if } \left(\frac{d_0}{p}\right)=1,\ p \text{ is represented by } K_p \text{ and } K_p = K_p^{-1}, \\ 0 & \text{if } p \text{ is not represented by } K_p. \end{cases}$$

(iii) *For $t \ge 2\alpha + 2$ we have*

$$R'(K, p^t) = \begin{cases} \varepsilon_k(t, m) W_{p^\alpha} & \text{if } \left(\frac{d_0}{p}\right) = 1,\ p \text{ is represented by } \\ & \qquad A \in H(d/p^{2\alpha}) \text{ and } K_p = A^k, \\ 0 & \text{otherwise,} \end{cases}$$

where m is the order of A in $H(d/p^{2\alpha})$ and $\varepsilon_k(t, m)$ is the number of elements in $\{k, -k\}$ which are congruent to $t - 2\alpha \pmod m$.

Proof. For $t = 1$, by Lemma 5.2(i) we know that $R'(K, p) = 0$ since $p \mid f$. Thus (i) holds for $t = 1$. Now assume $t \ge 2$. From Lemma 5.1 we have

$$R'(K, p^t) = R(K, p^t) - R(K, p^{t-2}).$$

If $t \le 2\alpha$ and $2 \nmid t$, then $R(K, p^t) = R(K, p^{t-2}) = 0$ by Theorem 5.3(i). Thus $R'(K, p^t) = 0$. If $t \le 2\alpha$ and $2 \mid t$, observing that $R'(K, p^t) \ge 0$ and then applying Theorem 5.3(i) and (5.1) we obtain (i).

For $t = 2\alpha + 1$, by the above and Theorem 5.3 we obtain

$$\begin{aligned} R'(K, p^{2\alpha+1}) &= R(K, p^{2\alpha+1}) - R(K, p^{2\alpha-1}) = R(K, p^{2\alpha+1}) \\ &= \begin{cases} R(K_p, p) & \text{if } d < 0, \\ W_{p^\alpha} R(K_p, p) & \text{if } d > 0. \end{cases} \end{aligned}$$

Since $K_p \in H(d/p^{2\alpha})$ and $f(d/p^{2\alpha}) = f/p^\alpha \not\equiv 0 \pmod p$, applying the above and Lemma 5.2 we see that (ii) holds.

As for $t \ge 2\alpha + 2$, from Lemma 5.1 and Theorem 5.3(ii) we have

$$\begin{aligned} R'(K, p^t) &= R(K, p^t) - R(K, p^{t-2}) \\ &= \begin{cases} R(K_p, p^{t-2\alpha}) - R(K_p, p^{t-2-2\alpha}) = R'(K_p, p^{t-2\alpha}) & \text{if } d < 0, \\ W_{p^\alpha}(R(K_p, p^{t-2\alpha}) - R(K_p, p^{t-2-2\alpha})) = W_{p^\alpha} R'(K_p, p^{t-2\alpha}) & \\ & \text{if } d > 0. \end{cases} \end{aligned}$$

Now recalling that $p \nmid \frac{f}{p^\alpha}$ and applying Theorem 5.2 we obtain (iii).

Summarizing the above we prove the theorem.

THEOREM 5.5. *Let d be a discriminant with conductor f. Let p be a prime such that $\left(\frac{d}{p}\right) = 0, 1$ and $p \nmid f$. Then p is represented by some class $A \in H(d)$. For $t \in \mathbb{N}$ and $K \in H(d)$ we have*

$$R(K, p^{t+1}) + R(K, p^{t-1}) = R(AK, p^t) + R(A^{-1}K, p^t).$$

Proof. We first assume $p \mid d$. By Lemma 5.2, p is represented by exactly one class A in $H(d)$ and $A = A^{-1}$. If $A = I$, by Theorem 5.1(ii) we have $R(I, p^t) = w(d)$ and $R(K, p^t) = 0$ for $K \ne I$, thus the result is true. If

$A \neq I$, by Theorem 5.1(ii) we have

$$R(I,p^t)=\begin{cases} w(d) & \text{if } 2\,|\,t, \\ 0 & \text{if } 2\nmid t, \end{cases} \quad R(A,p^t)=\begin{cases} 0 & \text{if } 2\,|\,t, \\ w(d) & \text{if } 2\nmid t, \end{cases}$$

and $R(K,p^t)=0$ for $K \neq I, A$. Using this we can easily check the result.

Now suppose $\left(\frac{d}{p}\right)=1$. Let m be the order of A in $H(d)$. If K is not a power of A, then clearly AK and $A^{-1}K$ are not powers of A. From Theorem 5.1(iii) we see that $R(K,p^{t+1})=R(K,p^{t-1})=0$ and $R(AK,p^t)=R(A^{-1}K,p^t)=0$. So the result is true in this case.

Now suppose $K=A^k$ for some $k\in\mathbb{Z}$. From (5.5) we see that

$$\begin{aligned}
\frac{1}{w(d)}\left(R(K,p^{t+1})+R(K,p^{t-1})\right) &= \frac{1}{w(d)}\left(R(A^k,p^{t+1})+R(A^k,p^{t-1})\right) \\
&= \sum_{\substack{0\le r\le (t+1)/2 \\ t-2r\equiv k-1 \pmod m}} 1 + \sum_{\substack{0\le r< (t+1)/2 \\ t-2r\equiv -k-1 \pmod m}} 1 \\
&\quad + \sum_{\substack{0\le r\le (t-1)/2 \\ t-2r\equiv k+1 \pmod m}} 1 + \sum_{\substack{0\le r< (t-1)/2 \\ t-2r\equiv 1-k \pmod m}} 1 \\
&= \sum_{\substack{0\le r\le t/2 \\ t-2r\equiv k-1 \pmod m}} 1 + \sum_{\substack{0\le r< t/2 \\ t-2r\equiv -k-1 \pmod m}} 1 \\
&\quad + \sum_{\substack{0\le r\le t/2 \\ t-2r\equiv k+1 \pmod m}} 1 + \sum_{\substack{0\le r< t/2 \\ t-2r\equiv 1-k \pmod m}} 1 \\
&= \sum_{\substack{0\le r\le t/2 \\ t-2r\equiv k+1 \pmod m}} 1 + \sum_{\substack{0\le r< t/2 \\ t-2r\equiv -k-1 \pmod m}} 1 \\
&\quad + \sum_{\substack{0\le r\le t/2 \\ t-2r\equiv k-1 \pmod m}} 1 + \sum_{\substack{0\le r< t/2 \\ t-2r\equiv 1-k \pmod m}} 1 \\
&= \frac{1}{w(d)}\left(R(A^{k+1},p^t)+R(A^{k-1},p^t)\right) \\
&= \frac{1}{w(d)}\left(R(AK,p^t)+R(A^{-1}K,p^t)\right).
\end{aligned}$$

This completes the proof.

Corollary 5.1. *Suppose all the assumptions in Theorem* 5.5 *hold. Let H be a subgroup of $H(d)$. Then*

$$R(KH,p^{t+1})+R(KH,p^{t-1})=R(AKH,p^t)+R(A^{-1}KH,p^t).$$

6. The formula for $R(G, n)$ ($G \in G(d)$). Let d be a discriminant. The purpose of this section is to determine $R(G, n)$ when $G \in G(d)$ and $n \in \mathbb{N}$.

THEOREM 6.1. *Let d be a discriminant with conductor f, $d_0 = d/f^2$ and $n \in \mathbb{N}$. If (n, f^2) is not a square, or there exists a prime p such that $2 \nmid \mathrm{ord}_p\, n$ and $\left(\frac{d_0}{p}\right) = -1$, then $R(G, n) = 0$ for any $G \in G(d)$. Suppose $(n, f^2) = m^2$ for $m \in \mathbb{N}$ and $\left(\frac{d_0}{p}\right) = 0, 1$ for every prime p with $2 \nmid \mathrm{ord}_p\, n$. Then there are exactly $2^{t(d)-t(d/m^2)}$ genera G representing n, and for such a genus G we have $R(G, n) = N(n, d)/2^{t(d)-t(d/m^2)}$. Moreover, if k and n' are given by*

$$k = \prod_{p \mid d_0,\, 2 \nmid \mathrm{ord}_p\, n} p \quad \textit{and} \quad n' = \prod_{p \nmid d_0} p^{\mathrm{ord}_p(n/m^2)},$$

where p runs over all distinct prime divisors of n/m^2, then n' is represented by some class $[ak, bk, c] \in H(d/m^2)$ with $a, b, c \in \mathbb{Z}$ and $(a, km) = (c, k) = 1$. Set $H_0 = H^2(d) \cap \mathrm{Ker}\, \varphi_{1,m}$ and $\mathrm{Ker}\, \varphi_{1,m}/H_0 = \{A_1 H_0, \ldots, A_s H_0\}$. Then all the distinct genera of $H(d)$ representing n are $A_1 K H^2(d), \ldots, A_s K H^2(d)$, where $K = [a, bkm, ckm^2]$.

Proof. If (n, f^2) is not a square, or there exists a prime such that $2 \nmid \mathrm{ord}_p\, n$ and $\left(\frac{d_0}{p}\right) = -1$, by Theorem 4.1 we have $N(n, d) = 0$ and so $R(G, n) = 0$ for any $G \in G(d)$. Now suppose $(n, f^2) = m^2$ for $m \in \mathbb{N}$ and $\left(\frac{d_0}{p}\right) = 0, 1$ for every prime p with $2 \nmid \mathrm{ord}_p\, n$. It follows from Theorem 4.1 that $N(n, d) > 0$. Applying Corollary 3.4 we see that $N(n', d/m^2) > 0$. Thus using the fact that $(k, f/m) = 1$ and Theorem 2.4(ii) we see that n' is represented by some class $[ak, bk, c] \in H(d/m^2)$ with $a, b, c \in \mathbb{Z}$ and $(a, km) = (c, k) = 1$. Suppose $[ak, bk, c] \in G'$ for $G' \in G(d/m^2)$. Then $R(G', n') > 0$. Since $(n', d/m^2) = 1$, from genus theory we know that G' is the unique genus of $H(d/m^2)$ representing n' (see e.g. [KW2, Lemma 1]). For $K = [a, bkm, ckm^2]$ we have $\varphi_{k,m}(K) = [ak, bk, c]$. By Corollary 3.5, Lemma 2.6 and the above we see that for $G \in G(d)$, $R(G, n) > 0$ if and only if $\varphi_{k,m}(G) = G'$. Now the result follows from Corollaries 2.3 and 3.5.

REMARK 6.1. This theorem extends a result of Kaplan and Williams [KW2], who showed that there are exactly $2^{t(d)-t(d/M^2)}$ genera G representing n provided $(n/M^2,\ f/M) = 1$ and $N(n, d) > 0$, where M is the largest integer such that $M^2 \mid n$ and $M \mid f$.

If $|G(d)| = 2$ and $G \in G(d)$, it follows from Theorem 6.1 that $R(G, n) = 0, N(n, d)$ or $N(n, d)/2$. Thus we have

COROLLARY 6.1. *Let d be a discriminant such that $|G(d)| = 2$, say $G(d) = \{G, G'\}$. Then for $n \in \mathbb{N}$ we have*

$$R(G, n) R(G', n) (R(G, n) - R(G', n)) = 0.$$

7. Multiplicative functions involving $R(K,n)$. For a discriminant d let $K \in H(d)$. For $n \in \mathbb{N}$ let $R(K,n)$ and $R'(K,n)$ be defined by Definition 3.2. The purpose of this section is to give multiplicative functions involving $R(K,n)$.

THEOREM 7.1. *Let d be a discriminant. If $n_1,\dots,n_r$ $(r \ge 2)$ are pairwise prime positive integers and $K \in H(d)$, then*

$$R(K,n_1\cdots n_r) = \frac{1}{w(d)^{r-1}} \sum_{K_1\cdots K_r=K} R(K_1,n_1)\cdots R(K_r,n_r),$$

$$R'(K,n_1\cdots n_r) = \frac{1}{w(d)^{r-1}} \sum_{K_1\cdots K_r=K} R'(K_1,n_1)\cdots R'(K_r,n_r),$$

where the summations are taken over all $K_1,\dots,K_r \in H(d)$ such that $K_1\cdots K_r = K$.

Proof. For $K \in H(d)$ and $n \in \mathbb{N}$ let $H_K(n)$ be defined by Definition 3.1. Recently Muzaffar and Williams ([MW2, Lemma 5.5]) showed that for $d<0$, if $n_1,n_2 \in \mathbb{N}$ and $(n_1,n_2)=1$, then

$$H_K(n_1n_2) = \sum_{K_1K_2=K} H_{K_1}(n_1)H_{K_2}(n_2), \tag{7.1}$$

where the summation is taken over all $K_1,K_2 \in H(d)$ such that $K_1K_2=K$. For $B \in \mathbb{Z}$ with $0 \le B < 2n_1n_2$ and $B^2 \equiv d \pmod{4n_1n_2}$, in the proof of (7.1) Muzaffar and Williams used the fact that

$$[n_1n_2,B,(B^2-d)/(4n_1n_2)] = [n_1,B,(B^2-d)/(4n_1)][n_2,B,(B^2-d)/(4n_2)].$$

This fact is easily deduced from Lemma 2.4. Checking their proof of (7.1) we find (7.1) is also valid when $d>0$. Using Theorem 3.1 and (7.1) we see that

$$\begin{aligned}\frac{R(K,n_1n_2)}{w(d)} &= \sum_{m^2\mid n_1n_2} H_K\Big(\frac{n_1n_2}{m^2}\Big) = \sum_{m_1^2\mid n_1}\sum_{m_2^2\mid n_2} H_K\Big(\frac{n_1}{m_1^2}\cdot\frac{n_2}{m_2^2}\Big)\\ &= \sum_{m_1^2\mid n_1}\sum_{m_2^2\mid n_2}\sum_{\substack{K_1,K_2\in H(d)\\ K_1K_2=K}} H_{K_1}\Big(\frac{n_1}{m_1^2}\Big)H_{K_2}\Big(\frac{n_2}{m_2^2}\Big)\\ &= \sum_{\substack{K_1,K_2\in H(d)\\ K_1K_2=K}} \sum_{m_1^2\mid n_1} H_{K_1}\Big(\frac{n_1}{m_1^2}\Big)\sum_{m_2^2\mid n_2} H_{K_2}\Big(\frac{n_2}{m_2^2}\Big)\\ &= \sum_{\substack{K_1,K_2\in H(d)\\ K_1K_2=K}} \frac{R(K_1,n_1)}{w(d)}\cdot\frac{R(K_2,n_2)}{w(d)}.\end{aligned}$$

Thus the first result is true for $r=2$.

Now we prove the first result by induction. Suppose $r>2$ and that the result holds for $r-1$ pairwise prime positive integers. From the above and the inductive hypothesis we see that

$$R(K,n_1\cdots n_r)=\frac{1}{w(d)}\sum_{\substack{A,K_r\in H(d)\\ AK_r=K}}R(A,n_1\cdots n_{r-1})R(K_r,n_r)$$

$$=\frac{1}{w(d)}\sum_{\substack{A,K_r\in H(d)\\ AK_r=K}}\frac{R(K_r,n_r)}{w(d)^{r-2}}\sum_{\substack{K_1,\dots,K_{r-1}\in H(d)\\ K_1\cdots K_{r-1}=A}}R(K_1,n_1)\cdots R(K_{r-1},n_{r-1})$$

$$=\frac{1}{w(d)^{r-1}}\sum_{\substack{K_1,\dots,K_r\in H(d)\\ K_1\cdots K_r=K}}R(K_1,n_1)\cdots R(K_r,n_r).$$

The result for $R(K,n_1\cdots n_r)$ now follows by induction.

Observe that $R'(K,n)=w(d)H_K(n)$ by Theorem 3.1. Using (7.1) and induction one can similarly prove the remaining result for $R'(K,n_1\cdots n_r)$.

Definition 7.1. Let d be a discriminant and $n\in\mathbb{N}$. Let $H(d)=\{A_1^{k_1}\cdots A_r^{k_r}\mid 0\le k_1<h_1,\dots,0\le k_r<h_r\}$ with $h_1\cdots h_r=h(d)$. For $K=A_1^{k_1}\cdots A_r^{k_r}\in H(d)$ and $M=A_1^{m_1}\cdots A_r^{m_r}\in H(d)$ with $k_i,m_i\in\{0,1,\dots,h_i-1\}$ $(i=1,\dots,r)$ we define

$$[K,M]=\frac{k_1m_1}{h_1}+\cdots+\frac{k_rm_r}{h_r}$$

and

$$F(M,n)=\frac{1}{w(d)}\sum_{K\in H(d)}\cos 2\pi[K,M]\cdot R(K,n)$$
$$=\frac{1}{w(d)}\sum_{\substack{0\le k_1<h_1\\ \cdots\\ 0\le k_r<h_r}}\cos 2\pi\Big(\frac{k_1m_1}{h_1}+\cdots+\frac{k_rm_r}{h_r}\Big)\cdot R(A_1^{k_1}\cdots A_r^{k_r},n).$$

Remark 7.1. Let d be a discriminant and $K,M\in H(d)$. By (5.1) we have $R(K,1)=w(d)$ or 0 according as $K=I$ or $K\ne I$. Thus $F(M,1)=1$ by Definition 7.1. From Definition 7.1 we also know that $F(M,n)=F(M^{-1},n)$ for $n\in\mathbb{N}$ and

$$F(I,n)=\frac{1}{w(d)}\sum_{K\in H(d)}R(K,n)=\frac{1}{w(d)}N(n,d).$$

By Theorem 4.1, if (n,f^2) is not a square or there is a prime p such that $\big(\frac{d_0}{p}\big)=-1$ and $2\nmid \operatorname{ord}_p n$, then we have $N(n,d)=0$, $R(K,n)=0$ and hence $F(M,n)=0$.

THEOREM 7.2. *Let d be a discriminant and $n \in \mathbb{N}$.*

(i) *If $M \in H(d)$, then $F(M,n)$ is a multiplicative function of n.*
(ii) *If $K \in H(d)$, then*

$$R(K,n) = \frac{w(d)}{h(d)} \sum_{M \in H(d)} \cos 2\pi[K,M] \cdot F(M,n).$$

Proof. Since $R(K,n) = R(K^{-1},n)$ we see that

$$\begin{aligned} F(M,n) &= \frac{1}{w(d)} \sum_{K \in H(d)} \cos 2\pi[K,M] \cdot R(K,n) \\ &= \frac{1}{2w(d)} \sum_{K \in H(d)} (e^{2\pi i[K,M]} + e^{-2\pi i[K,M]}) R(K,n) \\ &= \frac{1}{2w(d)} \sum_{K \in H(d)} (e^{2\pi i[K,M]} R(K,n) + e^{2\pi i[K^{-1},M]} R(K^{-1},n)) \\ &= \frac{1}{w(d)} \sum_{K \in H(d)} e^{2\pi i[K,M]} R(K,n). \end{aligned}$$

Similarly, as $F(M,n) = F(M^{-1},n)$ we have

$$\sum_{M \in H(d)} \cos 2\pi[K,M] \cdot F(M,n) = \sum_{M \in H(d)} e^{2\pi i[K,M]} F(M,n).$$

Let $n_1, n_2 \in \mathbb{N}$ and $(n_1,n_2) = 1$. For $K, L, M \in H(d)$ it is easily seen that $e^{2\pi i[KL,M]} = e^{2\pi i[K,M]} \cdot e^{2\pi i[L,M]}$ and

$$\sum_{M \in H(d)} e^{2\pi i[KL,M]} = \begin{cases} h(d) & \text{if } L = K^{-1}, \\ 0 & \text{if } L \neq K^{-1}. \end{cases}$$

From Theorem 7.1 and the above we have

$$\begin{aligned} &F(M, n_1 n_2) \\ &\quad = \frac{1}{w(d)} \sum_{K \in H(d)} e^{2\pi i[K,M]} R(K, n_1 n_2) \\ &\quad = \frac{1}{w(d)^2} \sum_{K \in H(d)} e^{2\pi i[K,M]} \sum_{\substack{K_1, K_2 \in H(d) \\ K_1 K_2 = K}} R(K_1,n_1) R(K_2,n_2) \\ &\quad = \frac{1}{w(d)^2} \sum_{K \in H(d)} \sum_{\substack{K_1, K_2 \in H(d) \\ K_1 K_2 = K}} e^{2\pi i[K_1,M]} \cdot e^{2\pi i[K_2,M]} R(K_1,n_1) R(K_2,n_2) \end{aligned}$$

$$= \frac{1}{w(d)^2}\sum_{K_1\in H(d)}\sum_{K_2\in H(d)} e^{2\pi i[K_1,M]}R(K_1,n_1)\cdot e^{2\pi i[K_2,M]}R(K_2,n_2)$$

$$= \frac{1}{w(d)^2}\Big(\sum_{K_1\in H(d)} e^{2\pi i[K_1,M]}R(K_1,n_1)\Big)\Big(\sum_{K_2\in H(d)} e^{2\pi i[K_2,M]}R(K_2,n_2)\Big)$$

$$= F(M,n_1)F(M,n_2).$$

Thus (i) is true.

Now we consider (ii). By the above, it is clear that

$$\frac{w(d)}{h(d)}\sum_{M\in H(d)}\cos 2\pi[K,M]\cdot F(M,n)$$
$$= \frac{w(d)}{h(d)}\sum_{M\in H(d)} e^{2\pi i[K,M]}F(M,n)$$
$$= \frac{w(d)}{h(d)}\sum_{M\in H(d)} e^{2\pi i[K,M]}\cdot\frac{1}{w(d)}\sum_{L\in H(d)} e^{2\pi i[L,M]}R(L,n)$$
$$= \frac{1}{h(d)}\sum_{L\in H(d)}\Big(\sum_{M\in H(d)} e^{2\pi i[KL,M]}\Big)R(L,n)$$
$$= R(K^{-1},n) = R(K,n).$$

So the theorem is proved.

Remark 7.2. Let d be a discriminant and $n\in\mathbb{N}$. If we define

$$F'(M,n) = \frac{1}{w(d)}\sum_{K\in H(d)}\cos 2\pi[K,M]\cdot R'(K,n) \quad \text{for } M\in H(d),$$

in a similar way we can show that $F'(M,n)$ is a multiplicative function of n and

$$R'(K,n) = \frac{w(d)}{h(d)}\sum_{M\in H(d)}\cos 2\pi[K,M]\cdot F'(M,n) \quad \text{for } K\in H(d).$$

From Theorem 7.2 we have

Theorem 7.3. *Let d be a discriminant such that $H(d)$ is cyclic and $h(d)=h$. Let I be the principal class in $H(d)$, and let A be a generator of $H(d)$. Set $\Delta_h = 1$ or 0 according as $2\mid h$ or $2\nmid h$. Then for any $m\in\mathbb{Z}$,*

$$F(A^m,n)$$
$$= \frac{1}{w(d)}\Big(\sum_{1\le k<h/2} 2\cos\frac{2\pi km}{h}\,R(A^k,n) + R(I,n) + (-1)^m\Delta_h R(A^{h/2},n)\Big)$$

is a multiplicative function of n. *Moreover*, *for* $k \in \mathbb{Z}$ *we have*

$$R(A^k, n) = \frac{w(d)}{h}\Big(\sum_{1\le m<h/2} 2\cos\frac{2\pi km}{h}\, F(A^m, n) + F(I, n) + (-1)^k \Delta_h F(A^{h/2}, n)\Big).$$

Proof. For $K \in H(d)$, by Remark 3.1 we have $R(K, n) = R(K^{-1}, n)$. Thus $R(A^k, n) = R(A^{h-k}, n)$ for $1 \le k < h/2$. Hence, from Definition 7.1 and Theorem 7.2(i) we see that

$$\begin{aligned} F(A^m, n) &= \frac{1}{w(d)} \sum_{0\le k<h} \cos\frac{2\pi km}{h}\, R(A^k, n) \\ &= \frac{1}{w(d)}\Big(\sum_{1\le k<h/2} 2\cos\frac{2\pi km}{h}\, R(A^k, n) + R(I, n) + (-1)^m \Delta_h R(A^{h/2}, n)\Big) \end{aligned}$$

is a multiplicative function of n. Similarly, from the fact that $F(A^m, n) = F(A^{h-m}, n)$ and Theorem 7.2(ii) we obtain the remaining result.

Theorem 7.4. *Let* d *be a discriminant such that* $H(d)$ *is cyclic and* $2 \le h(d) \le 6$ ($h(d) \in \{2, 3, 5, 6\}$ *implies* $H(d)$ *is cyclic*). *Let* I *be the principal class in* $H(d)$. *Let* A *be a generator of* $H(d)$ *and* $n \in \mathbb{N}$. *Recall that* $w(d) = 1$ *or* 2 *according as* $d > 0$ *or* $d < 0$.

(i) *If* $h(d) = 2, 3$, *then* $F(A, n) = (R(I, n) - R(A, n))/w(d)$ *is a multiplicative function of* n.

(ii) *If* $h(d) = 4$, *then*

$$F(A, n) = (R(I, n) - R(A^2, n))/w(d),$$
$$F(A^2, n) = (R(I, n) + R(A^2, n) - 2R(A, n))/w(d)$$

are multiplicative functions of n.

(iii) *If* $h(d) = 5$, *then*

$$F(A, n) = \Big(R(I, n) + \frac{\sqrt{5}-1}{2} R(A, n) - \frac{\sqrt{5}+1}{2} R(A^2, n)\Big)/w(d),$$
$$F(A^2, n) = \Big(R(I, n) - \frac{\sqrt{5}+1}{2} R(A, n) + \frac{\sqrt{5}-1}{2} R(A^2, n)\Big)/w(d)$$

are multiplicative functions of n.

(iv) *If* $h(d) = 6$, *then*

$$F(A, n) = (R(I, n) + R(A, n) - R(A^2, n) - R(A^3, n))/w(d),$$
$$F(A^2, n) = (R(I, n) - R(A, n) - R(A^2, n) + R(A^3, n))/w(d),$$
$$F(A^3, n) = (R(I, n) - 2R(A, n) + 2R(A^2, n) - R(A^3, n))/w(d)$$

are multiplicative functions of n.

Proof. Observe that

$$\cos\frac{2\pi}{3}=-\frac{1}{2},\quad \cos\frac{2\pi}{4}=0,\quad \cos\frac{2\pi}{6}=\frac{1}{2},\quad \cos\frac{4\pi}{6}=-\frac{1}{2},$$
$$\cos\frac{2\pi}{5}=\sin\frac{\pi}{10}=\frac{\sqrt{5}-1}{4},\quad \cos\frac{4\pi}{5}=-\cos\frac{\pi}{5}=-\frac{\sqrt{5}+1}{4}.$$

Putting $h=2,3,4,5,6$ in Theorem 7.3 we obtain the result.

REMARK 7.3. Putting $h=8,10,12$ in Theorem 7.3 one can obtain the results similar to Theorem 7.4. For example, if $H(d)=\{I,A,\dots,A^7\}$ with $A^8=I$, then $F(A^2,n)=(R(I,n)-2R(A^2,n)+R(A^4,n))/w(d)$ is a multiplicative function of $n\in\mathbb{N}$.

8. Formulas for $F(M,p^t)$. Let d be a discriminant and $M\in H(d)$. The purpose of this section is to determine $F(M,p^t)$, where p is a prime and $t\in\mathbb{N}$. From now on we let $R(M)$ denote the set of integers represented by $M\in H(d)$.

Let $\{U_n(x)\}$ be the Chebyshev polynomials of the second kind given by

$$U_0(x)=1,\quad U_1(x)=2x,\quad U_{n+1}(x)=2xU_n(x)-U_{n-1}(x)\quad (n\ge 1). \tag{8.1}$$

It is well known that (see [MOS])

$$U_n(1)=n+1,\quad U_n(-1)=(-1)^n(n+1), \tag{8.2}$$

$$U_n(\cos\theta)=\frac{\sin(n+1)\theta}{\sin\theta}\quad (\theta\ne 0,\pm\pi,\pm2\pi,\dots) \tag{8.3}$$

and

$$\begin{aligned} U_n(x)&=\sum_{r=0}^{[n/2]}(-1)^r\binom{n-r}{r}(2x)^{n-2r}\\ &=\sum_{s=0}^{[n/2]}\binom{n+1}{2s+1}x^{n-2s}(x^2-1)^s. \end{aligned} \tag{8.4}$$

THEOREM 8.1. *Let d be a discriminant with conductor f. Let $H(d)=\{A_1^{k_1}\cdots A_r^{k_r}\mid 0\le k_1<h_1,\dots,0\le k_r<h_r\}$ with $h_1\cdots h_r=h(d)$. Let $M=A_1^{m_1}\cdots A_r^{m_r}\in H(d)$. Let p be a prime not dividing f and let t be a nonnegative integer.*

(i) *If $\left(\frac{d}{p}\right)=-1$, then*

$$F(M,p^t)=\begin{cases}1 & \text{if } 2\mid t,\\ 0 & \text{if } 2\nmid t.\end{cases}$$

(ii) *If* $p \mid d$, *then* p *is represented by exactly one class* $A \in H(d)$ *and* $A = A_1^{\varepsilon_1 h_1/2} \cdots A_r^{\varepsilon_r h_r/2}$ *with* $\varepsilon_1, \ldots, \varepsilon_r \in \{0,1\}$, *and*

$$F(M, p^t) = (-1)^{(\varepsilon_1 m_1 + \cdots + \varepsilon_r m_r)t}.$$

(iii) *If* $\left(\frac{d}{p}\right) = 1$ *so that* p *is represented by some class* $A = A_1^{a_1} \cdots A_r^{a_r} \in H(d)$, *then*

$$F(M, p^t) = U_t(\cos 2\pi(a_1 m_1/h_1 + \cdots + a_r m_r/h_r))$$

$$= \begin{cases} (-1)^{2t(a_1 m_1/h_1 + \cdots + a_r m_r/h_r)}(t+1) \\ \qquad\qquad \text{if } 2(a_1 m_1/h_1 + \cdots + a_r m_r/h_r) \in \mathbb{Z}, \\ \dfrac{\sin 2\pi(a_1 m_1/h_1 + \cdots + a_r m_r/h_r)(t+1)}{\sin 2\pi(a_1 m_1/h_1 + \cdots + a_r m_r/h_r)} \\ \qquad\qquad \text{if } 2(a_1 m_1/h_1 + \cdots + a_r m_r/h_r) \notin \mathbb{Z}. \end{cases}$$

Proof. If $\left(\frac{d}{p}\right) = -1$, by Theorem 5.1(i) we have for $K \in H(d)$,

$$R(K, p^t) = \begin{cases} w(d) & \text{if } K = I \text{ and } 2 \mid t, \\ 0 & \text{otherwise.} \end{cases}$$

Thus, by Definition 7.1 we have

$$F(M, p^t) = \frac{1}{w(d)} R(I, p^t) = \frac{1 + (-1)^t}{2}.$$

This proves (i).

Now suppose $p \mid d$. From [MW2, Lemma 5.3] we know that p is represented by exactly one class $A \in H(d)$ and $A = A^{-1}$. Thus

$$A = A_1^{\varepsilon_1 h_1/2} \cdots A_r^{\varepsilon_r h_r/2} \quad \text{with } \varepsilon_1, \ldots, \varepsilon_r \in \{0,1\}.$$

Suppose $K \in H(d)$. If $A = I$, by Theorem 5.1(ii) we have $R(I, p^t) = w(d)$ and $R(K, p^t) = 0$ for $K \neq I$, thus $F(M, p^t) = 1$ by Definition 7.1. If $A \neq I$, by Theorem 5.1(ii) we have

$$R(I, p^t) = \frac{1 + (-1)^t}{2} w(d), \qquad R(A, p^t) = \frac{1 - (-1)^t}{2} w(d)$$

and $R(K, p^t) = 0$ for $K \neq I, A$. Thus

$$\begin{aligned} F(M, p^t) &= \frac{1 + (-1)^t}{2} + \frac{1 - (-1)^t}{2} \cos 2\pi\left(\frac{m_1 \varepsilon_1 h_1/2}{h_1} + \cdots + \frac{m_r \varepsilon_r h_r/2}{h_r}\right) \\ &= \frac{1 + (-1)^t}{2} + \frac{1 - (-1)^t}{2} (-1)^{\varepsilon_1 m_1 + \cdots + \varepsilon_r m_r} = (-1)^{(\varepsilon_1 m_1 + \cdots + \varepsilon_r m_r)t}. \end{aligned}$$

Finally, consider (iii). By Definition 7.1 and Theorem 5.5 we have for $t\in\mathbb{N}$,

$$\begin{aligned}F(M,p^{t+1})+F(M,p^{t-1})&=\frac{1}{w(d)}\sum_{K\in H(d)}\cos 2\pi[K,M]\cdot(R(K,p^{t+1})+R(K,p^{t-1}))\\&=\frac{1}{w(d)}\sum_{K\in H(d)}\cos 2\pi[K,M]\cdot(R(AK,p^{t})+R(A^{-1}K,p^{t}))\\&=\frac{1}{w(d)}\sum_{L\in H(d)}(\cos 2\pi[A^{-1}L,M]\cdot R(L,p^{t})+\cos 2\pi[AL,M]\cdot R(L,p^{t}))\\&=\frac{1}{w(d)}\sum_{L\in H(d)}2\cos 2\pi[A,M]\cos 2\pi[L,M]\cdot R(L,p^{t})\\&=2\cos 2\pi[A,M]\cdot F(M,p^{t}).\end{aligned}$$

Set $x=\cos 2\pi[A,M]$. Then

$$F(M,p^{t+1})=2xF(M,p^{t})-F(M,p^{t-1}). \tag{8.5}$$

From Remark 7.1 we have $F(M,1)=1$. Using Definition 7.1 and Lemma 5.2(iii) we see that $F(M,p)=2x$. Therefore

$$F(M,p^{t})=U_t(x)\quad \text{for } t=0,1,2,\ldots.$$

Now applying (8.2) and (8.3) yields the result. So the theorem is proved.

From Theorem 8.1 we have

Corollary 8.1. *Let d be a discriminant with conductor f. Suppose that $H(d)$ is cyclic with order h and generator A. Let p be a prime such that $p\nmid f$. Let t be a nonnegative integer and $s\in\mathbb{Z}$.*

(i) *If* $\left(\frac{d}{p}\right)=-1$, *then*

$$F(A^s,p^t)=\begin{cases}1 & \text{if } 2\mid t,\\ 0 & \text{if } 2\nmid t.\end{cases}$$

(ii) *If $p\mid d$, then p is represented by $A^{\varepsilon h/2}$ for unique $\varepsilon\in\{0,1\}$ and*

$$F(A^s,p^t)=(-1)^{\varepsilon st}.$$

(iii) *If* $\left(\frac{d}{p}\right)=1$ *so that p is represented by some class $A^a\in H(d)$, then*

$$F(A^s,p^t)=U_t(\cos 2\pi as/h)=\begin{cases}(-1)^{2ast/h}(t+1) & \text{if } 2as/h\in\mathbb{Z},\\[4pt] \dfrac{\sin 2\pi as(t+1)/h}{\sin 2\pi as/h} & \text{if } 2as/h\notin\mathbb{Z}.\end{cases}$$

From Corollary 8.1 we deduce

Corollary 8.2. *Let d be a discriminant such that $H(d)$ is a cyclic group of order h. Let p be a prime such that $\left(\frac{d}{p}\right)=1$ and p is represented by $A\in H(d)$. Let m be the order of A in $H(d)$. Let t_1 and t_2 be nonnegative integers such that $t_1\equiv t_2 \pmod m$. Then $F(M,p^{t_1})=F(M,p^{t_2})$ for any $M\in H(d)$ with $M^{\frac{h}{m/(2,m)}}\neq I$.*

Theorem 8.2 (Reduction Theorem for $F(M,n)$). *Let d be a discriminant with conductor f, and $H(d)=\{A_1^{k_1}\cdots A_r^{k_r}\mid 0\le k_1<h_1,\dots,0\le k_r<h_r\}$ with $h_1\cdots h_r=h(d)$. Let $M=A_1^{m_1}\cdots A_r^{m_r}\in H(d)$ and $n\in\mathbb{N}$.*

(i) *If (n,f^2) is not a square, then $F(M,n)=0$.*

(ii) *If $(n,f^2)=m^2$ for $m\in\mathbb{N}$ and $\operatorname{Ker}\varphi_{1,m}=\{A_1^{a_1n_1}\cdots A_r^{a_rn_r}\mid 0\le a_1<h_1/n_1,\dots,0\le a_r<h_r/n_r\}$ with $n_1\mid h_1,\dots,n_r\mid h_r$, then*

$$F(M,n)=\begin{cases} m\prod_{p\mid m}\left(1-\frac{1}{p}\left(\frac{d/m^2}{p}\right)\right)F\left(\varphi_{1,m}(A_1)^{\frac{m_1n_1}{h_1}}\cdots\varphi_{1,m}(A_r)^{\frac{m_rn_r}{h_r}},\frac{n}{m^2}\right) & \\ \qquad\qquad\qquad\qquad \text{if } h_j\mid m_jn_j \text{ for all } j=1,\dots,r, & \\ 0 \qquad\qquad\qquad\qquad \text{otherwise}, & \end{cases}$$

where in the product p runs over all distinct prime divisors of m.

Proof. If (n,f^2) is not a square, from Theorem 3.2 we have $R(K,n)=0$ for any K in $H(d)$. Thus $F(M,n)=0$ by Definition 7.1. This proves (i).

Now consider (ii). Suppose $(n,f^2)=m^2$ for $m\in\mathbb{N}$ and $\operatorname{Ker}\varphi_{1,m}=\{A_1^{a_1n_1}\cdots A_r^{a_rn_r}\mid 0\le a_1<h_1/n_1,\dots,0\le a_r<h_r/n_r\}$ with $n_1\mid h_1,\dots,n_r\mid h_r$. Let $c(d,m)$ be given by (3.4). Applying Theorems 3.2 and 2.1 we see that if $l_1,\dots,l_r,a_1,\dots,a_r$ are integers, then

$$\begin{aligned}R(A_1^{l_1+a_1n_1}\cdots A_r^{l_r+a_rn_r},n)&=c(d,m)R(\varphi_{1,m}(A_1^{l_1+a_1n_1}\cdots A_r^{l_r+a_rn_r}),n/m^2)\\&=c(d,m)R(\varphi_{1,m}(A_1^{l_1}\cdots A_r^{l_r}),n/m^2)\\&=c(d,m)R(\varphi_{1,m}(A_1)^{l_1}\cdots\varphi_{1,m}(A_r)^{l_r},n/m^2).\end{aligned}$$

Hence

$$\begin{aligned}&F(M,n)\\&=\frac{1}{w(d)}\sum_{\substack{0\le k_1<h_1\\ \cdots\\ 0\le k_r<h_r}}\cos 2\pi(k_1m_1/h_1+\dots+k_rm_r/h_r)\cdot R(A_1^{k_1}\cdots A_r^{k_r},n)\\&=\frac{1}{w(d)}\sum_{\substack{0\le l_1<n_1\\ \cdots\\ 0\le l_r<n_r}}\sum_{\substack{0\le a_1<h_1/n_1\\ \cdots\\ 0\le a_r<h_r/n_r}}\cos 2\pi((l_1+a_1n_1)m_1/h_1+\dots+(l_r+a_rn_r)m_r/h_r)\\&\quad\times R(A_1^{l_1+a_1n_1}\cdots A_r^{l_r+a_rn_r},n)\end{aligned}$$

$$= \frac{c(d,m)}{w(d)} \sum_{\substack{0\le l_1<n_1\\ \cdots\\ 0\le l_r<n_r}} R(\varphi_{1,m}(A_1)^{l_1}\cdots\varphi_{1,m}(A_r)^{l_r}, n/m^2)$$

$$\times \sum_{\substack{0\le a_1<h_1/n_1\\ \cdots\\ 0\le a_r<h_r/n_r}} \cos 2\pi((l_1+a_1n_1)m_1/h_1+\cdots+(l_r+a_rn_r)m_r/h_r).$$

Since

$$2 \sum_{\substack{0\le a_1<h_1/n_1\\ \cdots\\ 0\le a_r<h_r/n_r}} \cos 2\pi((l_1+a_1n_1)m_1/h_1+\cdots+(l_r+a_rn_r)m_r/h_r)$$

$$= \sum_{\substack{0\le a_1<h_1/n_1\\ \cdots\\ 0\le a_r<h_r/n_r}} \left(e^{2\pi i\sum_{j=1}^r (l_j+a_jn_j)m_j/h_j} + e^{-2\pi i\sum_{j=1}^r (l_j+a_jn_j)m_j/h_j}\right)$$

$$= e^{2\pi i\sum_{j=1}^r l_jm_j/h_j} \sum_{\substack{0\le a_1<h_1/n_1\\ \cdots\\ 0\le a_r<h_r/n_r}} e^{2\pi i\sum_{j=1}^r a_jn_jm_j/h_j}$$

$$+ e^{-2\pi i\sum_{j=1}^r l_jm_j/h_j} \sum_{\substack{0\le a_1<h_1/n_1\\ \cdots\\ 0\le a_r<h_r/n_r}} e^{-2\pi i\sum_{j=1}^r a_jn_jm_j/h_j}$$

$$= e^{2\pi i\sum_{j=1}^r l_jm_j/h_j} \prod_{j=1}^r \Big(\sum_{a_j=0}^{h_j/n_j-1} e^{2\pi i a_jn_jm_j/h_j}\Big)$$

$$+ e^{-2\pi i\sum_{j=1}^r l_jm_j/h_j} \prod_{j=1}^r \Big(\sum_{a_j=0}^{h_j/n_j-1} e^{-2\pi i a_jn_jm_j/h_j}\Big)$$

$$= \begin{cases} \dfrac{h_1\cdots h_r}{n_1\cdots n_r}\left(e^{2\pi i\sum_{j=1}^r l_jm_j/h_j} + e^{-2\pi i\sum_{j=1}^r l_jm_j/h_j}\right) & \text{if } h_1\mid m_1n_1,\ldots,h_r\mid m_rn_r,\\ 0 & \text{otherwise} \end{cases}$$

$$= \begin{cases} \dfrac{h_1\cdots h_r}{n_1\cdots n_r}\cdot 2\cos 2\pi(l_1m_1/h_1+\cdots+l_rm_r/h_r) & \text{if } h_1\mid m_1n_1,\ldots,h_r\mid m_rn_r,\\ 0 & \text{otherwise,} \end{cases}$$

we see that if $h_j\nmid m_jn_j$ for some $j\in\{1,\ldots,r\}$, then $F(M,n)=0$; if

$h_j \mid m_j n_j$ for all $j = 1, \dots, r$, then

$$F(M,n) = \frac{c(d,m)}{w(d)} \sum_{\substack{0\le l_1<n_1\\ \cdots \\ 0\le l_r<n_r}} R(\varphi_{1,m}(A_1)^{l_1}\cdots\varphi_{1,m}(A_r)^{l_r}, n/m^2) \times \frac{h_1\cdots h_r}{n_1\cdots n_r}\cos 2\pi(l_1m_1/h_1+\cdots+l_rm_r/h_r).$$

As $\varphi_{1,m}$ is surjective from $H(d)$ to $H(d/m^2)$ and by the assumption $\operatorname{Ker}\varphi_{1,m} = \{A_1^{a_1n_1}\cdots A_r^{a_rn_r} \mid 0\le a_1<h_1/n_1,\dots,0\le a_r<h_r/n_r\}$, we see that

$$H(d/m^2) = \{\varphi_{1,m}(A_1)^{l_1}\cdots\varphi_{1,m}(A_r)^{l_r} \mid 0\le l_1<n_1,\dots,0\le l_r<n_r\}.$$

Therefore, if $m_jn_j/h_j \in \mathbb{Z}$ for all $j=1,\dots,r$, by the above and Definition 7.1 we have

$$\begin{aligned}F(M,n) &= \frac{c(d,m)h_1\cdots h_r w(d/m^2)}{n_1\cdots n_r w(d)}\cdot\frac{1}{w(d/m^2)}\sum_{\substack{0\le l_1<n_1\\ \cdots \\ 0\le l_r<n_r}}\cos\Big(2\pi\sum_{j=1}^r \frac{l_j}{n_j}\cdot\frac{m_jn_j}{h_j}\Big)\\ &\quad\times R(\varphi_{1,m}(A_1)^{l_1}\cdots\varphi_{1,m}(A_r)^{l_r}, n/m^2)\\ &= \frac{c(d,m)h_1\cdots h_r w(d/m^2)}{n_1\cdots n_r w(d)} F(\varphi_{1,m}(A_1)^{m_1n_1/h_1}\cdots\varphi_{1,m}(A_r)^{m_rn_r/h_r}, n/m^2).\end{aligned}$$

Since $H(d/m^2)\cong H(d)/\operatorname{Ker}\varphi_{1,m}$ by Theorem 2.1, we see that

$$\frac{h_1\cdots h_r}{n_1\cdots n_r} = |\operatorname{Ker}\varphi_{1,m}| = \frac{|H(d)|}{|H(d/m^2)|} = \frac{h(d)}{h(d/m^2)}.$$

Thus applying Lemma 3.5 we obtain

$$\frac{c(d,m)h_1\cdots h_r w(d/m^2)}{n_1\cdots n_r w(d)} = \frac{c(d,m)h(d)w(d/m^2)}{h(d/m^2)w(d)} = m\prod_{p\mid m}\Big(1-\frac{1}{p}\Big(\frac{d/m^2}{p}\Big)\Big),$$

where p runs over all distinct prime divisors of m. Hence

$$\begin{aligned}F(M,n) &= m\prod_{p\mid m}\Big(1-\frac{1}{p}\Big(\frac{d/m^2}{p}\Big)\Big)F(\varphi_{1,m}(A_1)^{m_1n_1/h_1}\cdots\varphi_{1,m}(A_r)^{m_rn_r/h_r}, n/m^2).\end{aligned}$$

This proves (ii) and hence the proof is complete.

From Theorem 8.2 we have

THEOREM 8.3. *Let d be a discriminant with conductor f. Suppose $H(d)$ is cyclic with generator A and order h. Let $s\in\mathbb{Z}$ and $n\in\mathbb{N}$.*

(i) *If (n,f^2) is not a square, then $F(A^s,n)=0$.*

(ii) *If* $(n, f^2) = m^2$ *for* $m \in \mathbb{N}$ *and* $h' = h(d/m^2)$, *then* $h' \mid h$ *and*

$$F(A^s, n) = \begin{cases} m \prod_{p \mid m} \left(1 - \frac{1}{p}\left(\frac{d/m^2}{p}\right)\right) F(\varphi_{1,m}(A)^{sh'/h}, n/m^2) & \text{if } \frac{h}{h'} \mid s, \\ 0 & \text{if } \frac{h}{h'} \nmid s, \end{cases}$$

where p runs over all distinct prime divisors of m.

Proof. If (n, f^2) is not a square, by Theorem 8.2 we have $F(A^s, n) = 0$. If $(n, f^2) = m^2$ for $m \in \mathbb{N}$ and $h' = h(d/m^2)$, from Theorem 2.1 we know that $\operatorname{Ker} \varphi_{1,m}$ is a subgroup of $H(d)$ and $|\operatorname{Ker} \varphi_{1,m}| = h/h'$. Since $H(d)$ is cyclic with generator A, $\operatorname{Ker} \varphi_{1,m}$ must be generated by A^j for some $j \in \mathbb{N}$. Let (A^i) be the subgroup generated by A^i; clearly $|(A^i)| = h/(i, h)$. Thus

$$h/(j, h) = |(A^j)| = |\operatorname{Ker} \varphi_{1,m}| = h/h' = |(A^{h'})|.$$

Hence $(j, h) = h'$ and so $h' \mid j$. Therefore $(A^j) \subseteq (A^{h'})$ and so $(A^j) = (A^{h'})$. Thus $\operatorname{Ker} \varphi_{1,m} = (A^j) = (A^{h'})$. Now the result follows from Theorem 8.2.

THEOREM 8.4. *Let d be a discriminant with conductor f and $d_0 = d/f^2$. Suppose $H(d)$ is cyclic with order h and generator A. Let p be a prime such that $p \mid f$ and $p^\alpha \parallel f$. Let $s \in \mathbb{Z}$ and $t \in \mathbb{N}$.*

(i) *If* $t < 2\alpha$ *and* $2 \nmid t$, *then* $F(A^s, p^t) = 0$.

(ii) *If* $t < 2\alpha$ *and* $2 \mid t$, *then*

$$F(A^s, p^t) = \begin{cases} p^{t/2} & \text{if } h \mid sh(d/p^t), \\ 0 & \text{if } h \nmid sh(d/p^t). \end{cases}$$

(iii) *Suppose* $t \geq 2\alpha$ *and* $h \nmid sh(d/p^{2\alpha})$. *Then* $F(A^s, p^t) = 0$.

(iv) *Suppose* $t \geq 2\alpha$, $h \mid sh(d/p^{2\alpha})$ *and* $\left(\frac{d_0}{p}\right) = -1$. *Then*

$$F(A^s, p^t) = \begin{cases} p^{\alpha-1}(p+1) & \text{if } 2 \mid t, \\ 0 & \text{if } 2 \nmid t. \end{cases}$$

(v) *Suppose* $t \geq 2\alpha$, $h \mid sh(d/p^{2\alpha})$ *and* $p \mid d_0$. *Let I_p be the principal class in $H(d/p^{2\alpha})$. Then*

$$F(A^s, p^t) = \begin{cases} p^\alpha & \text{if } p \text{ is represented by } I_p, \\ (-1)^{(st/h)h(d/p^{2\alpha})} p^\alpha & \text{if } p \text{ is not represented by } I_p. \end{cases}$$

(vi) *Suppose* $t \geq 2\alpha$, $h \mid sh(d/p^{2\alpha})$ *and* $\left(\frac{d_0}{p}\right) = 1$. *Then p is represented by $\varphi_{1,p^\alpha}(A)^r$ for some $r \in \mathbb{Z}$, and*

$$F(A^s, p^t) = \begin{cases} (-1)^{2rst/h}(t - 2\alpha + 1) p^{\alpha-1}(p-1) & \text{if } 2rs/h \in \mathbb{Z}, \\ \dfrac{\sin 2\pi rs(t - 2\alpha + 1)/h}{\sin 2\pi rs/h} p^{\alpha-1}(p-1) & \text{if } 2rs/h \notin \mathbb{Z}. \end{cases}$$

Proof. If $t < 2\alpha$ and $2\nmid t$, then $(p^t, f^2) = p^t$ is not a square and so $F(A^k, p^t) = 0$ by Theorem 8.3(i). This proves (i).

Now consider (ii). If $t < 2\alpha$ and $2 \mid t$, then $(p^t, f^2) = (p^{t/2})^2$. Thus applying Theorem 8.3(ii) and Remark 7.1 we see that

$$F(A^s, p^t) = \begin{cases} p^{t/2} F(\varphi_{1,p^{t/2}}(A)^{sh(d/p^t)/h}, 1) = p^{t/2} & \text{if } h \mid sh(d/p^t), \\ 0 & \text{if } h \nmid sh(d/p^t). \end{cases}$$

Thus (ii) holds.

Now suppose $t \ge 2\alpha$ and $h_p = h(d/p^{2\alpha})$. Then $(p^t, f^2) = p^{2\alpha}$. If $h \nmid sh_p$, by Theorem 8.3(ii) we have $F(A^s, p^t) = 0$. Thus (iii) is true. From now on we assume $h \mid sh_p$. Set $A_p = \varphi_{1,p^\alpha}(A)$. Then A_p is a generator of $H(d/p^{2\alpha})$ by Theorem 2.1. From the above and Theorem 8.3(ii) we have

$$F(A^s, p^t) = p^\alpha \left(1 - \frac{1}{p}\left(\frac{d_0}{p}\right)\right) F(A_p^{sh_p/h}, p^{t-2\alpha}). \tag{8.6}$$

If $\left(\frac{d_0}{p}\right) = -1$, applying Corollary 8.1(i) we obtain

$$F(A^s, p^t) = p^{\alpha-1}(p+1) F(A_p^{sh_p/h}, p^{t-2\alpha}) = \begin{cases} p^{\alpha-1}(p+1) & \text{if } 2 \mid t, \\ 0 & \text{if } 2 \nmid t. \end{cases}$$

This proves (iv). If $p \mid d_0$, by the above and Corollary 8.1(ii) we have

$$\begin{aligned} F(A^s, p^t) &= p^\alpha F(A_p^{sh_p/h}, p^{t-2\alpha}) \\ &= \begin{cases} p^\alpha & \text{if } p \text{ is represented by } I_p, \\ (-1)^{(sh_p/h)(t-2\alpha)} p^\alpha & \text{if } p \text{ is not represented by } I_p. \end{cases} \end{aligned}$$

So (v) holds.

Finally consider the case $t \ge 2\alpha$, $h \mid sh_p$ and $\left(\frac{d_0}{p}\right) = 1$. Since A_p is a generator of $H(d/p^{2a})$ and $\left(\frac{d/p^{2\alpha}}{p}\right) = \left(\frac{d_0}{p}\right) = 1$, p must be represented by A_p^r for some integer r. By Corollary 8.1(iii) we get

$$F(A_p^{sh_p/h}, p^{t-2\alpha}) = \begin{cases} (-1)^{2(t-2\alpha)rs/h}(t - 2\alpha + 1) & \text{if } 2rs/h \in \mathbb{Z}, \\ \dfrac{\sin 2\pi rs(t-2\alpha+1)/h}{\sin 2\pi rs/h} & \text{if } 2rs/h \notin \mathbb{Z}. \end{cases}$$

This together with (8.6) proves (vi). So the theorem is proved.

Putting $h(d) = 2$ and $s = 1$ in Corollary 8.1 and Theorem 8.4 we deduce

Theorem 8.5. *Let d be a discriminant with conductor f and $d_0 = d/f^2$. Suppose $h(d) = 2$ and $H(d) = \{I, A\}$ with $A^2 = I$. For $n \in \mathbb{N}$ let $F(A, n) = (R(I, n) - R(A, n))/w(d)$. Let p be a prime and let t be a nonnegative integer.*

(i) *If $p\nmid f$, then*

$$F(A,p^t)=\begin{cases}\frac12(1+(-1)^t) & \text{if } \left(\frac{d_0}{p}\right)=-1,\\ 1 & \text{if } p\mid d_0 \text{ and } p\in R(I),\\ (-1)^t & \text{if } p\mid d_0 \text{ and } p\in R(A),\\ t+1 & \text{if } p\nmid d_0 \text{ and } p\in R(I),\\ (-1)^t(t+1) & \text{if } p\nmid d_0 \text{ and } p\in R(A).\end{cases}$$

(ii) *If $p\mid f$, say $p^\alpha \parallel f$, setting $h_p=h(d/p^{2\alpha})$ we then have*

$$F(A,p^t)=\begin{cases}p^{t/2} & \text{if } t<2\alpha,\ 2\mid t \text{ and } h(d/p^t)=2,\\ p^{\alpha-1}(p+1) & \text{if } t\ge 2\alpha,\ 2\mid t,\ h_p=2 \text{ and } \left(\frac{d_0}{p}\right)=-1,\\ p^\alpha & \text{if } t\ge 2\alpha,\ h_p=2,\ p\mid d_0 \text{ and } p\in R(I_p),\\ (-1)^t p^\alpha & \text{if } t\ge 2\alpha,\ h_p=2,\ p\mid d_0 \text{ and } p\notin R(I_p),\\ (t-2\alpha+1)(p^\alpha-p^{\alpha-1}) & \\ & \text{if } t\ge 2\alpha,\ h_p=2,\ p\nmid d_0 \text{ and } p\in R(I_p),\\ (-1)^t(t-2\alpha+1)(p^\alpha-p^{\alpha-1}) & \\ & \text{if } t\ge 2\alpha,\ h_p=2,\ p\nmid d_0 \text{ and } p\in R(A_p),\\ 0 & \text{otherwise},\end{cases}$$

where I_p is the principal class in $H(d/p^{2\alpha})$ and A_p is a generator of $H(d/p^{2\alpha})$.

Suppose $h(d)=3$. If p is a prime such that $p\mid d$ and $p\nmid f(d)$, from Corollary 8.1(ii) we know that p is represented by the principal class I in $H(d)$. Thus applying Corollary 8.1 and Theorem 8.4 we have

THEOREM 8.6. *Let d be a discriminant with conductor f and $d_0=d/f^2$. Suppose $h(d)=3$ and $H(d)=\{I,A,A^2\}$ with $A^3=I$. For $n\in\mathbb{N}$ let $F(A,n)=(R(I,n)-R(A,n))/w(d)$. Let p be a prime and let t be a non-negative integer.*

(i) *If $p\nmid f$, then*

$$F(A,p^t)=\begin{cases}1 & \text{if } p\mid d_0,\\ \frac12(1+(-1)^t) & \text{if } \left(\frac{d_0}{p}\right)=-1,\\ t+1 & \text{if } p\nmid d_0 \text{ and } p\in R(I),\\ -1 & \text{if } p\in R(A) \text{ and } t\equiv 1 \pmod 3,\\ 0 & \text{if } p\in R(A) \text{ and } t\equiv 2 \pmod 3,\\ 1 & \text{if } p\in R(A) \text{ and } t\equiv 0 \pmod 3.\end{cases}$$

(ii) *If* $p \mid f$, *say* $p^\alpha \parallel f$, *setting* $h_p = h(d/p^{2\alpha})$ *we then have*

$$F(A,p^t)=\begin{cases} p^{t/2} & \text{if } t<2\alpha,\ 2\mid t \text{ and } h(d/p^t)=3,\\ p^{\alpha-1}(p+1) & \text{if } t\ge 2\alpha,\ 2\mid t,\ h_p=3 \text{ and } \left(\frac{d_0}{p}\right)=-1,\\ p^\alpha & \text{if } t\ge 2\alpha,\ h_p=3 \text{ and } p\mid d_0,\\ (t-2\alpha+1)p^{\alpha-1}(p-1) & \\ & \text{if } t\ge 2\alpha,\ h_p=3,\ p\nmid d_0 \text{ and } p\in R(I_p),\\ p^{\alpha-1}(p-1) & \text{if } t\ge 2\alpha,\ h_p=3,\ p\in R(A_p)\\ & \quad \text{and } t-2\alpha\equiv 0 \pmod 3,\\ -p^{\alpha-1}(p-1) & \text{if } t\ge 2\alpha,\ h_p=3,\ p\in R(A_p)\\ & \quad \text{and } t-2\alpha\equiv 1 \pmod 3,\\ 0 & \text{otherwise,} \end{cases}$$

where I_p *is the principal class in* $H(d/p^{2\alpha})$ *and* A_p *is a generator of* $H(d/p^{2\alpha})$.

Suppose $h(d)=4$. From Corollary 8.1 we have

Theorem 8.7. *Let* d *be a discriminant with conductor* f *and* $d_0 = d/f^2$. *Suppose* $h(d)=4$ *and* $H(d)=\{I,A,A^2,A^3\}$ *with* $A^4=I$. *Let*

$$F(A,n)=\frac{1}{w(d)}\,(R(I,n)-R(A^2,n)),$$
$$F(A^2,n)=\frac{1}{w(d)}\,(R(I,n)+R(A^2,n)-2R(A,n))$$

for $n\in\mathbb{N}$. *Let* p *be a prime such that* $p\nmid f$ *and let* t *be a nonnegative integer. Then*

$$F(A,p^t)=\begin{cases} (1+(-1)^t)/2 & \text{if } \left(\frac{d_0}{p}\right)=-1,\\ 1 & \text{if } p\mid d_0 \text{ and } p\in R(I),\\ t+1 & \text{if } p\nmid d_0 \text{ and } p\in R(I),\\ (-1)^t & \text{if } p\mid d_0 \text{ and } p\in R(A^2),\\ (-1)^t(t+1) & \text{if } p\nmid d_0 \text{ and } p\in R(A^2),\\ (-1)^{t/2} & \text{if } p\in R(A) \text{ and } 2\mid t,\\ 0 & \text{if } p\in R(A) \text{ and } 2\nmid t \end{cases}$$

and

$$F(A^2,p^t)=\begin{cases} (1+(-1)^t)/2 & \text{if } \left(\frac{d_0}{p}\right)=-1,\\ 1 & \text{if } p\mid d_0,\\ t+1 & \text{if } p\nmid d_0 \text{ and } p\in R(I)\cup R(A^2),\\ (-1)^t(t+1) & \text{if } p\in R(A). \end{cases}$$

9. Formulas for $R(K,n)$ $(K\in H(d))$ when $h(d)=2$. Throughout this section p denotes a prime and products (sums) over p run through all distinct primes p satisfying any restrictions given under the product (summation) symbol.

LEMMA 9.1. *Let d be a discriminant such that $H(d)$ is cyclic and $h(d)=2,4$. If $m\in\mathbb{N}$ and $m\mid f(d)$, then $h(d/m^2)=1$ if and only if $t(d/m^2)=0$, and $h(d/m^2)>1$ if and only if $t(d/m^2)=1$.*

Proof. Since $h(d/m^2)\mid h(d)$ by Remark 2.2, we see that

$$h\Big(\frac{d}{m^2}\Big)=1 \ \Leftrightarrow\ \Big|G\Big(\frac{d}{m^2}\Big)\Big|=2^{t(d/m^2)}=1 \ \Leftrightarrow\ t\Big(\frac{d}{m^2}\Big)=0$$

and

$$h\Big(\frac{d}{m^2}\Big)>1 \ \Leftrightarrow\ \Big|G\Big(\frac{d}{m^2}\Big)\Big|=2^{t(d/m^2)}=2 \ \Leftrightarrow\ t\Big(\frac{d}{m^2}\Big)=1.$$

This proves the lemma.

THEOREM 9.1. *Let d be a discriminant with conductor f and $d_0=d/f^2$. Suppose $h(d)=2$ and $H(d)=\{I,A\}$ with $A^2=I$. Let $n\in\mathbb{N}$ and $F(A,n)=(R(I,n)-R(A,n))/w(d)$. Let $N(n,d)$ be as in Theorem 4.1.*

(i) *If (n,f^2) is not a square, then $R(I,n)=R(A,n)=0$ and $F(A,n)=0$.*
(ii) *If $(n,f^2)=m^2$ for $m\in\mathbb{N}$ and $h(d/m^2)=1$ (i.e. $t(d/m^2)=0$), then $R(I,n)=R(A,n)=N(n,d)/2$ and $F(A,n)=0$.*
(iii) *If $(n,f^2)=m^2$ for $m\in\mathbb{N}$ and $h(d/m^2)=2$ (i.e. $t(d/m^2)=1$), then*

$$R(I,n)=N(n,d)-R(A,n)=\frac{1+(-1)^s}{2}\,N(n,d)$$

and

$$F(A,n)=(-1)^sN(n,d)/w(d),$$

where $s=\sum_{p\in R(A_0)}\operatorname{ord}_p n$, A_0 is the generator of $H(d/m^2)$ and p runs over all distinct primes satisfying $p\in R(A_0)$.

Proof. From Theorems 8.3, 3.4 and Lemma 9.1 we know that (i) and (ii) hold. Now consider (iii). Suppose $(n,f^2)=m^2$ for $m\in\mathbb{N}$ and $h(d/m^2)=2$. Set $n_0=n/m^2$ and $H(d/m^2)=\{I_0,A_0\}$ with $A_0^2=I_0$. By Theorem 2.1 we have $\varphi_{1,m}(A)=A_0$. Thus using Theorem 8.3 we have

$$F(A,n)=m\prod_{p\mid m}\bigg(1-\frac{1}{p}\Big(\frac{d/m^2}{p}\Big)\bigg)F(A_0,n_0).$$

Clearly $d/m^2=d_0(f/m)^2$, $(n_0,(f/m)^2)=1$ and $f(d/m^2)=f/m$. Thus, if p is a prime dividing n_0, then $p\nmid f/m$ and so $p\nmid f(d/m^2)$. Now applying Theorems 7.4(i) and 8.5(i) we obtain

$$\begin{aligned}F(A_0,n_0) &= \prod_p F(A_0,p^{\operatorname{ord}_p n_0})\\ &= \prod_{p\mid d_0,\, p\in R(A_0)} (-1)^{\operatorname{ord}_p n_0} \prod_{(\frac{d_0}{p})=-1} \frac{1+(-1)^{\operatorname{ord}_p n_0}}{2}\\ &\quad\times \prod_{p\nmid d_0,\, p\in R(I_0)} (1+\operatorname{ord}_p n_0) \prod_{p\nmid d_0,\, p\in R(A_0)} (-1)^{\operatorname{ord}_p n_0}(1+\operatorname{ord}_p n_0)\\ &= (-1)^s \prod_{(\frac{d_0}{p})=-1} \frac{1+(-1)^{\operatorname{ord}_p n}}{2} \prod_{(\frac{d_0}{p})=1} (1+\operatorname{ord}_p n_0),\end{aligned}$$

where p runs over all distinct prime divisors of n_0. Now combining the above with Lemma 9.1 and Theorem 4.1 yields $F(A,n) = (-1)^s N(n,d)/w(d)$. Note that $R(I,n) = (N(n,d)+w(d)F(A,n))/2$ and $R(A,n) = (N(n,d) - w(d)F(A,n))/2$. We then obtain the remaining result for $R(I,n)$ and $R(A,n)$. The proof is now complete.

Let d be a discriminant such that $h(d)=2$. For $d>0$, from [B, p. 31] we know that $h(d)=2$ for $d = 12, 21, 24, 28, 32, 33, 40, 44, 45, 48, \ldots$. It seems that there are infinitely many positive discriminants d such that $h(d)=2$.

Now we illustrate that there are exactly 29 negative discriminants d with $h(d)=2$. We first recall that if $D<0$ is a fundamental discriminant, then

$$h(D)=1 \iff D = -3,-4,-7,-8,-11,-19,-43,-67,-163 \tag{9.1}$$

and

$$\begin{aligned}h(D)=2 \iff D = {}&-15,-20,-24,-35,-40,-51,-52,\\ &-88,-91,-115,-123,-148,-187,\\ &-232,-235,-267,-403,-427,\end{aligned} \tag{9.2}$$

see for example [C, p. 234]. From [Cox, p. 149] we also know that if $d<0$ is a discriminant, then

$$\begin{aligned}h(d)=1 \iff d = {}&-3,-4,-7,-8,-11,-12,-16,-19,\\ &-27,-28,-43,-67,-163.\end{aligned} \tag{9.3}$$

We now determine those discriminants $d<0$ such that $h(d)=2$. Suppose $d<0$ is a discriminant with conductor f and $d_0 = d/f^2$. By (9.2), it suffices to determine those discriminants $d<0$ with $h(d)=2$ and $f>1$. Since $h(d)=2$ we have $d<-4$ and so $w(d)=2$. By Lemma 3.5 we obtain

$$f\prod_{p\mid f}\Big(1-\frac{1}{p}\Big(\frac{d_0}{p}\Big)\Big) = \frac{w(d_0)}{h(d_0)} = \begin{cases} 6 & \text{if } d_0=-3,\\ 4 & \text{if } d_0=-4,\\ 2 & \text{if } d_0<-4 \text{ and } h(d_0)=1,\\ 1 & \text{if } h(d_0)=2.\end{cases} \tag{9.4}$$

From this we see that $d_0=-3$ implies $f=4,5,7$ and so $d=-48,-75,-147$, and $d_0=-4$ implies $f=3,4,5$ and so $d=-36,-64,-100$. If $d_0<-4$ and $h(d_0)=1$, then $f=2,3,4$ and d_0 satisfies $2\mid d_0$, $d_0\equiv 1 \pmod 3$, $d_0\equiv 1 \pmod 8$ according as $f=2,3,4$. Since $d_0<-4$ and $h(d_0)=1$ if and only if $d_0= -7,-8,-11,-19,-43,-67,-163$ we must have $d=-32,-72,-99,-112$. Now suppose $h(d_0)=2$. Then d_0 is given by (9.2). If $h(d_0)=2$ and $f>1$, we must have $f=2$ and $d_0\equiv 1 \pmod 8$. This yields $d_0=-15$ and so $d=-60$. Thus there are exactly 29 values of $d<0$ such that $h(d)=2$.

Table 9.1

d	I	Conditions for $p\in R(I)$	A	Conditions for $p\in R(A)$
-15	$[1,1,4]$	$p\equiv 1,4 \pmod{15}$	$[2,1,2]$	$p=3,5,\ p\equiv 2,8 \pmod{15}$
-20	$[1,0,5]$	$p=5,\ p\equiv 1,9 \pmod{20}$	$[2,2,3]$	$p=2,\ p\equiv 3,7 \pmod{20}$
-24	$[1,0,6]$	$p\equiv 1,7 \pmod{24}$	$[2,0,3]$	$p=2,3,\ p\equiv 5,11 \pmod{24}$
-32	$[1,0,8]$	$p\equiv 1 \pmod 8$	$[3,2,3]$	$p\equiv 3 \pmod 8$
-35	$[1,1,9]$	$(\frac{p}{5})=(\frac{p}{7})=1$	$[3,1,3]$	$p=5,7,\ (\frac{p}{5})=(\frac{p}{7})=-1$
-36	$[1,0,9]$	$p\equiv 1 \pmod{12}$	$[2,2,5]$	$p=2,\ p\equiv 5 \pmod{12}$
-40	$[1,0,10]$	$(\frac{-2}{p})=(\frac{p}{5})=1$	$[2,0,5]$	$p=2,5,\ (\frac{-2}{p})=(\frac{p}{5})=-1$
-48	$[1,0,12]$	$p\equiv 1 \pmod{12}$	$[3,0,4]$	$p=3,\ p\equiv 7 \pmod{12}$
-51	$[1,1,13]$	$(\frac{p}{3})=(\frac{p}{17})=1$	$[3,3,5]$	$p=3,17,\ (\frac{p}{3})=(\frac{p}{17})=-1$
-52	$[1,0,13]$	$p=13,\ (\frac{-1}{p})=(\frac{p}{13})=1$	$[2,2,7]$	$p=2,\ (\frac{-1}{p})=(\frac{p}{13})=-1$
-60	$[1,0,15]$	$p\equiv 1,19 \pmod{30}$	$[3,0,5]$	$p=3,5,\ p\equiv 17,23 \pmod{30}$
-64	$[1,0,16]$	$p\equiv 1 \pmod 8$	$[4,4,5]$	$p\equiv 5 \pmod 8$
-72	$[1,0,18]$	$p\equiv 1,19 \pmod{24}$	$[2,0,9]$	$p=2,\ p\equiv 11,17 \pmod{24}$
-75	$[1,1,19]$	$p\equiv 1,4 \pmod{15}$	$[3,3,7]$	$p=3,\ p\equiv 7,13 \pmod{15}$
-88	$[1,0,22]$	$(\frac{2}{p})=(\frac{p}{11})=1$	$[2,0,11]$	$p=2,11,\ (\frac{2}{p})=(\frac{p}{11})=-1$
-91	$[1,1,23]$	$(\frac{p}{7})=(\frac{p}{13})=1$	$[5,3,5]$	$p=7,13,\ (\frac{p}{7})=(\frac{p}{13})=-1$
-99	$[1,1,25]$	$(\frac{p}{3})=(\frac{p}{11})=1$	$[5,1,5]$	$p=11,\ (\frac{p}{3})=-(\frac{p}{11})=-1$
-100	$[1,0,25]$	$p\equiv 1,9 \pmod{20}$	$[2,2,13]$	$p=2,\ p\equiv 13,17 \pmod{20}$
-112	$[1,0,28]$	$(\frac{-1}{p})=(\frac{p}{7})=1$	$[4,0,7]$	$p=7,\ (\frac{-1}{p})=-(\frac{p}{7})=-1$
-115	$[1,1,29]$	$(\frac{p}{5})=(\frac{p}{23})=1$	$[5,5,7]$	$p=5,23,\ (\frac{p}{5})=(\frac{p}{23})=-1$
-123	$[1,1,31]$	$(\frac{p}{3})=(\frac{p}{41})=1$	$[3,3,11]$	$p=3,41,\ (\frac{p}{3})=(\frac{p}{41})=-1$
-147	$[1,1,37]$	$(\frac{p}{3})=(\frac{p}{7})=1$	$[3,3,13]$	$p=3,\ (\frac{p}{3})=-(\frac{p}{7})=1$
-148	$[1,0,37]$	$p=37,\ (\frac{-1}{p})=(\frac{p}{37})=1$	$[2,2,19]$	$p=2,\ (\frac{-1}{p})=(\frac{p}{37})=-1$
-187	$[1,1,47]$	$(\frac{p}{11})=(\frac{p}{17})=1$	$[7,3,7]$	$p=11,17,\ (\frac{p}{11})=(\frac{p}{17})=-1$
-232	$[1,0,58]$	$(\frac{-2}{p})=(\frac{p}{29})=1$	$[2,0,29]$	$p=2,29,\ (\frac{-2}{p})=(\frac{p}{29})=-1$
-235	$[1,1,59]$	$(\frac{p}{5})=(\frac{p}{47})=1$	$[5,5,13]$	$p=5,47,\ (\frac{p}{5})=(\frac{p}{47})=-1$
-267	$[1,1,67]$	$(\frac{p}{3})=(\frac{p}{89})=1$	$[3,3,23]$	$p=3,89,\ (\frac{p}{3})=(\frac{p}{89})=-1$
-403	$[1,1,101]$	$(\frac{p}{13})=(\frac{p}{31})=1$	$[11,9,11]$	$p=13,31,\ (\frac{p}{13})=(\frac{p}{31})=-1$
-427	$[1,1,107]$	$(\frac{p}{7})=(\frac{p}{61})=1$	$[7,7,17]$	$p=7,61,\ (\frac{p}{7})=(\frac{p}{61})=-1$

LEMMA 9.2. *Let $d<0$ be a discriminant. Then $h(d)=2$ if and only if d is one of the* 29 *numbers listed in Table* 9.1. *If $h(d)=2$ and $H(d)=$*

$\{I,A\}$ with $A^2=I$, then I and A are given by Table 9.1, *and a prime p is represented by I or A depending on the corresponding congruence conditions in Table* 9.1.

THEOREM 9.2. *Let $d<0$ be a discriminant with conductor f and $d_0 = d/f^2$. Suppose $h(d)=2$, $H(d)=\{I,A\}$, $n\in\mathbb{N}$ and $F(A,n)=(R(I,n)-R(A,n))/2$.*

(i) *If there is a prime p with $2\nmid \operatorname{ord}_p n$ and $\left(\frac{d_0}{p}\right)=-1$, then $F(A,n)=0$.*

(ii) *Suppose $d=-60$ and $\left(\frac{-15}{p}\right)=0,1$ for every prime p with $2\nmid \operatorname{ord}_p n$. Assume $n=3^\alpha n_0$ $(3\nmid n_0)$. Then*

$$F(A,n)=F([3,0,5],n)$$
$$=\begin{cases}(-1)^\alpha\left(\dfrac{n_0}{3}\right)\displaystyle\prod_{(\frac{-15}{p})=1}(1+\operatorname{ord}_p n) & \text{if } 2\nmid n,\\ (-1)^\alpha\left(\dfrac{n_0}{3}\right)\displaystyle\prod_{(\frac{-15}{p})=1}\left(1+\operatorname{ord}_p \frac{n}{4}\right) & \text{if } 4\mid n,\\ 0 & \text{if } 2\parallel n.\end{cases}$$

(iii) *Suppose $d\neq -60$ and $\left(\frac{d_0}{p}\right)=0,1$ for every prime p with $2\nmid \operatorname{ord}_p n$. Then*

$$F(A,n)=\begin{cases}\chi(n,d)\displaystyle\prod_{(\frac{d_0}{p})=1}(1+\operatorname{ord}_p n) & \text{if } (n,f)=1,\\ 0 & \text{if } (n,f)>1,\end{cases}$$

where $\chi(n,d)$ is given by Table 9.2.

Table 9.2

d	f	$\chi(n,d)$ $((n,f)=1)$	d	f	$\chi(n,d)$ $((n,f)=1)$
-15	1	$(-1)^\alpha(\frac{n_0}{3})$ $(n=3^\alpha n_0, 3\nmid n_0)$	-91	1	$(-1)^\alpha(\frac{n_0}{7})$ $(n=7^\alpha n_0, 7\nmid n_0)$
-20	1	$(\frac{n_0}{5})$ $(n=5^\alpha n_0, 5\nmid n_0)$	-99	3	$(\frac{n}{3})$
-24	1	$(-1)^\alpha(\frac{n_0}{3})$ $(n=3^\alpha n_0, 3\nmid n_0)$	-100	5	$(\frac{n}{5})$
-32	2	$(\frac{-1}{n})$	-112	4	$(\frac{-1}{n})$
-35	1	$(-1)^\alpha(\frac{n_0}{5})$ $(n=5^\alpha n_0, 5\nmid n_0)$	-115	1	$(-1)^\alpha(\frac{n_0}{5})$ $(n=5^\alpha n_0, 5\nmid n_0)$
-36	3	$(\frac{n}{3})$	-123	1	$(-1)^\alpha(\frac{n_0}{3})$ $(n=3^\alpha n_0, 3\nmid n_0)$
-40	1	$(-1)^\alpha(\frac{n_0}{5})$ $(n=5^\alpha n_0, 5\nmid n_0)$	-147	7	$(\frac{n}{7})$
-48	4	$(\frac{-1}{n})$	-148	1	$(-1)^{\alpha+\frac{n_0-1}{2}}$ $(n=2^\alpha n_0, 2\nmid n_0)$
-51	1	$(-1)^\alpha(\frac{n_0}{3})$ $(n=3^\alpha n_0, 3\nmid n_0)$	-187	1	$(-1)^\alpha(\frac{n_0}{11})$ $(n=11^\alpha n_0, 11\nmid n_0)$
-52	1	$(\frac{n_0}{13})$ $(n=13^\alpha n_0, 13\nmid n_0)$	-232	1	$(-1)^\alpha(\frac{-2}{n_0})$ $(n=2^\alpha n_0, 2\nmid n_0)$
-64	4	$(\frac{n}{2})$	-235	1	$(-1)^\alpha(\frac{n_0}{5})$ $(n=5^\alpha n_0, 5\nmid n_0)$
-72	3	$(\frac{n}{3})$	-267	1	$(-1)^\alpha(\frac{n_0}{3})$ $(n=3^\alpha n_0, 3\nmid n_0)$
-75	5	$(\frac{n}{5})$	-403	1	$(-1)^\alpha(\frac{n_0}{13})$ $(n=13^\alpha n_0, 13\nmid n_0)$
-88	1	$(-1)^\alpha(\frac{2}{n_0})$ $(n=2^\alpha n_0, 2\nmid n_0)$	-427	1	$(-1)^\alpha(\frac{n_0}{7})$ $(n=7^\alpha n_0, 7\nmid n_0)$

Proof. From Remark 7.1 we see that (i) holds. From now on suppose $(\frac{d_0}{p})=0,1$ for every prime p with $2\nmid \operatorname{ord}_p n$. Let us consider (ii). Assume $d=-60$ and $n=3^\alpha n_0$ $(3\nmid n_0)$. Clearly $d_0=-15$, $f=2$, $I=[1,0,15]$, $A=[3,0,5]$ and $(n,f^2)=(n,4)=1,2,4$. If $2\,\|\,n$, then $(n,f^2)=2$ and so $F(A,n)=0$ by Theorem 9.1. If $2\nmid n$, then $(n,f^2)=1$. Putting $m=1$, $d_0=-15$ and $A=[3,0,5]$ in Theorem 9.1(iii) we obtain

$$F(A,n)=(-1)^{\sum_{p\in R([3,0,5])}\operatorname{ord}_p n}\prod_{(\frac{-15}{p})=1}(1+\operatorname{ord}_p n).$$

For any odd prime p, clearly $p\in R([3,0,5])$ if and only if $p=3,5$ or $p\equiv 2,8 \pmod{15}$ (see Table 9.1). Since $\left(\frac{-15}{p}\right)=-1$ implies $2\mid \operatorname{ord}_p n$ and $\left(\frac{-15}{p}\right)=0,1$ if and only if $p=3,5$ or $p\equiv 1,2,4,8 \pmod{15}$, we see that

$$n_0=N^2\prod_{p\equiv 1,4\,(\mathrm{mod}\,15)}p^{\operatorname{ord}_p n}\prod_{p\equiv 2,5,8\,(\mathrm{mod}\,15)}p^{\operatorname{ord}_p n},$$

where N is an integer coprime to 15. So

$$n_0\equiv 1 \pmod 3 \iff \sum_{p\equiv 2,5,8\,(\mathrm{mod}\,15)}\operatorname{ord}_p n\equiv 0 \pmod 2.$$

Hence

$$(-1)^\alpha\left(\frac{n_0}{3}\right)=(-1)^{\sum_{p\equiv 2,3,5,8\,(\mathrm{mod}\,15)}\operatorname{ord}_p n}=(-1)^{\sum_{p\in R([3,0,5])}\operatorname{ord}_p n}.$$

Therefore,

$$F(A,n)=(-1)^\alpha\left(\frac{n_0}{3}\right)\prod_{(\frac{-15}{p})=1}(1+\operatorname{ord}_p n).$$

If $4\mid n$, then $(n,f^2)=4$. Since $H(-15)=\{[1,1,4],[2,1,2]\}$ and $p\in R([2,1,2])$ if and only if $p=3,5$ or $p\equiv 2,8 \pmod{15}$ by Table 9.1, putting $m=2$ in Theorem 9.1(iii) and applying the above we find

$$\begin{aligned}F(A,n)&=(-1)^{\sum_{p\in R([2,1,2])}\operatorname{ord}_p n}\cdot 2\left(1-\frac12\left(\frac{-15}{2}\right)\right)\prod_{(\frac{-15}{p})=1}\left(1+\operatorname{ord}_p\frac n4\right)\\&=(-1)^{\sum_{p\equiv 2,3,5,8\,(\mathrm{mod}\,15)}\operatorname{ord}_p n}\prod_{(\frac{-15}{p})=1}\left(1+\operatorname{ord}_p\frac n4\right)\\&=(-1)^\alpha\left(\frac{n_0}{3}\right)\prod_{(\frac{-15}{p})=1}\left(1+\operatorname{ord}_p\frac n4\right).\end{aligned}$$

This proves (ii).

Now we consider (iii). Assume $d\ne -60$. If (n,f^2) is not a square, then $F(A,n)=0$ by Theorem 9.1(i). If $(n,f^2)=m^2$ for $m\in\{2,3,4,\dots\}$, from

Table 9.2 and (9.3) we see that $h(d/m^2) = 1$ and thus $F(A, n) = 0$ by Theorem 9.1(ii). Hence, if $(n, f) > 1$ (i.e. $(n, f^2) > 1$), then $F(A, n) = 0$.

Now suppose $(n, f) = 1$. By Theorem 9.1(iii) we have

$$F(A, n) = (-1)^{\sum_{p\in R(A)} \operatorname{ord}_p n} \prod_{(\frac{d_0}{p})=1} (1 + \operatorname{ord}_p n).$$

Thus it suffices to show that

$$\chi(n, d) = (-1)^{\sum_{p\in R(A)} \operatorname{ord}_p n}. \tag{9.5}$$

For a prime p, $p \mid (d, n)$ implies $p \nmid f$ since $(n, f) = 1$. So $p \in R(I)$ or $p \in R(A)$ by Corollary 4.2. As $(n, f) = 1$ and $2 \mid \operatorname{ord}_p n$ when $\left(\frac{d}{p}\right) = -1$ we see that

$$n = N^2 \prod_{p\in R(I)} p^{\operatorname{ord}_p n} \prod_{p\in R(A)} p^{\operatorname{ord}_p n}, \tag{9.6}$$

where $N = \prod_{(\frac{d}{p})=-1} p^{(\operatorname{ord}_p n)/2}$ is an integer coprime to d.

For $d \in \{-15, -20, -24, -35, -36, -40, -51, -52, -64, -72, -75, -91, -99, -100, -115, -123, -147, -187, -235, -267, -403, -427\}$, by Table 9.1 we can select a prime divisor q of d such that for any prime $p \neq q$,

$$p \in R(A) \Rightarrow \left(\frac{p}{q}\right) = -1 \quad \text{and} \quad p \in R(I) \Rightarrow \left(\frac{p}{q}\right) = 1.$$

Assume $n = q^\alpha n_0$ $(q \nmid n_0)$. Since

$$n_0 = N^2 \prod_{\substack{p\in R(I)\\ p\neq q}} p^{\operatorname{ord}_p n} \prod_{\substack{p\in R(A)\\ p\neq q}} p^{\operatorname{ord}_p n},$$

we see that

$$\begin{aligned}\left(\frac{n_0}{q}\right) &= \left(\frac{N^2}{q}\right) \prod_{\substack{p\in R(I)\\ p\neq q}} \left(\frac{p}{q}\right)^{\operatorname{ord}_p n} \prod_{\substack{p\in R(A)\\ p\neq q}} \left(\frac{p}{q}\right)^{\operatorname{ord}_p n} \\ &= \prod_{\substack{p\in R(A)\\ p\neq q}} (-1)^{\operatorname{ord}_p n} = (-1)^{\sum_{p\in R(A),\, p\neq q} \operatorname{ord}_p n}.\end{aligned}$$

Thus

$$(-1)^{\sum_{p\in R(A)} \operatorname{ord}_p n} = \begin{cases} (-1)^\alpha \left(\frac{n_0}{q}\right) & \text{if } q \in R(A), \\ \left(\frac{n_0}{q}\right) & \text{if } q \notin R(A). \end{cases}$$

This together with Tables 9.1 and 9.2 shows that (9.5) holds.

If $d\in\{-32,-48,-112\}$, then $f=2$ or 4 and so $2\nmid n$. From Table 9.1 and (9.6) we see that

$$n=N^2\prod_{\substack{p\in R(I)\\ p\equiv 1\,(\mathrm{mod}\,4)}}p^{\mathrm{ord}_p n}\prod_{\substack{p\in R(A)\\ p\equiv 3\,(\mathrm{mod}\,4)}}p^{\mathrm{ord}_p n}.$$

Therefore, $(n-1)/2\equiv\sum_{p\in R(A)}\mathrm{ord}_p n \pmod 2$. This yields (9.5).

If $d\in\{-88,-148,-232\}$ and $n=2^\alpha n_0$ $(2\nmid n_0)$, by Table 9.1 and (9.6) we have $2\in R(A)$ and

$$(-1)^{\sum_{p\in R(A)}\mathrm{ord}_p n}=(-1)^{\alpha+\sum_{p\in R(A)}\mathrm{ord}_p n_0}=\begin{cases}(-1)^\alpha\left(\frac{2}{n_0}\right) & \text{if } d=-88,\\ (-1)^\alpha\left(\frac{-1}{n_0}\right) & \text{if } d=-148,\\ (-1)^\alpha\left(\frac{-2}{n_0}\right) & \text{if } d=-232.\end{cases}$$

By the above, (9.5) holds and so (iii) is proved. Hence the proof is now complete.

THEOREM 9.3. *Let $d<0$ be a discriminant with conductor f and $d_0=d/f^2$. Suppose $h(d)=2$, $H(d)=\{I,A\}$ and $n\in\mathbb{N}$.*

(i) *If there is a prime p such that $2\nmid\mathrm{ord}_p n$ and $\left(\frac{d_0}{p}\right)=-1$, then $R(I,n)=R(A,n)=0$.*

(ii) *Suppose $d=-60$ and $\left(\frac{-15}{p}\right)=0,1$ for every prime p with $2\nmid\mathrm{ord}_p n$. Assume $n=3^\alpha n_0$ $(3\nmid n_0)$. Then*

$$R([1,0,15],n)=\begin{cases}\left(1+(-1)^\alpha\left(\frac{n_0}{3}\right)\right)\prod_{(\frac{-15}{p})=1}(1+\mathrm{ord}_p n) & \text{if } 2\nmid n,\\ \left(1+(-1)^\alpha\left(\frac{n_0}{3}\right)\right)\prod_{(\frac{-15}{p})=1}\left(1+\mathrm{ord}_p \frac{n}{4}\right) & \text{if } 4\mid n,\\ 0 & \text{if } 2\parallel n\end{cases}$$

and

$$R([3,0,5],n)=\begin{cases}\left(1-(-1)^\alpha\left(\frac{n_0}{3}\right)\right)\prod_{(\frac{-15}{p})=1}(1+\mathrm{ord}_p n) & \text{if } 2\nmid n,\\ \left(1-(-1)^\alpha\left(\frac{n_0}{3}\right)\right)\prod_{(\frac{-15}{p})=1}\left(1+\mathrm{ord}_p \frac{n}{4}\right) & \text{if } 4\mid n,\\ 0 & \text{if } 2\parallel n.\end{cases}$$

(iii) *Suppose* $d \neq -60$ *and* $\left(\frac{d_0}{p}\right) = 0, 1$ *for every prime* p *with* $2 \nmid \operatorname{ord}_p n$. *Then*

$$R(I,n) = \begin{cases} (1+\chi(n,d)) \prod_{(\frac{d_0}{p})=1} (1+\operatorname{ord}_p n) & \text{if } (n,f)=1, \\ w\left(\frac{d}{m^2}\right) \prod_{(\frac{d_0}{p})=1} \left(1+\operatorname{ord}_p \frac{n}{m^2}\right) & \\ \qquad\qquad\qquad\qquad \text{if } (n,f^2)=m^2 \text{ for } m \in \{2,3,4,\ldots\}, \\ 0 & \text{if } (n,f^2) \text{ is not a square} \end{cases}$$

and

$$R(A,n) = \begin{cases} (1-\chi(n,d)) \prod_{(\frac{d_0}{p})=1} (1+\operatorname{ord}_p n) & \text{if } (n,f)=1, \\ w\left(\frac{d}{m^2}\right) \prod_{(\frac{d_0}{p})=1} \left(1+\operatorname{ord}_p \frac{n}{m^2}\right) & \\ \qquad\qquad\qquad\qquad \text{if } (n,f^2)=m^2 \text{ for } m \in \{2,3,4,\ldots\}, \\ 0 & \text{if } (n,f^2) \text{ is not a square}, \end{cases}$$

where $\chi(n,d)$ *is given by Table* 9.2.

Proof. As $N(n,d) = R(I,n) + R(A,n)$ and $F(A,n) = \frac{1}{2}(R(I,n) - R(A,n))$ we have $R(I,n) = \frac{1}{2}N(n,d) + F(A,n)$ and $R(A,n) = \frac{1}{2}N(n,d) - F(A,n)$. By Lemma 3.5, Table 9.2 and (9.3) we see that if $m \in \mathbb{N}$ and $m \mid f$, then

$$w(d) \cdot m \prod_{p \mid m} \left(1 - \frac{1}{p}\left(\frac{d/m^2}{p}\right)\right) = \frac{h(d)w(d/m^2)}{h(d/m^2)} = \begin{cases} 2w(d/m^2) & \text{if } d \neq -60 \text{ and } m > 1, \\ w(d/m^2) = 2 & \text{if } d = -60 \text{ or } m = 1. \end{cases}$$

Now combining the above with Theorems 4.1 and 9.2 yields the result.

10. Formulas for $R(K,n)$ ($K \in H(d)$) when $h(d) = 3$

Theorem 10.1. *Let* d *be a discriminant with conductor* f *and* $d_0 = d/f^2$. *Suppose* $h(d) = 3$ *and* $H(d) = \{I, A, A^2\}$ *with* $A^3 = I$. *Let* $n \in \mathbb{N}$ *and* $F(A,n) = (R(I,n) - R(A,n))/w(d)$. *Let* $N(n,d)$ *be as in Theorem* 4.1.

(i) *If* (n,f^2) *is not a square, then* $R(I,n) = R(A,n) = R(A^2,n) = F(A,n) = 0$.

(ii) *If* $(n,f^2) = m^2$ *for* $m \in \mathbb{N}$ *and* $h(d/m^2) = 1$, *then* $R(I,n) = R(A,n) = R(A^2,n) = N(n,d)/3$ *and* $F(A,n) = 0$.

(iii) *Suppose* $(n,f^2)=m^2$ *for* $m\in\mathbb{N}$ *and* $h(d/m^2)=3$. *If there is a prime* p *such that* $\left(\frac{d_0}{p}\right)=-1$ *and* $2\nmid \operatorname{ord}_p n$, *then*

$$R(I,n)=R(A,n)=R(A^2,n)=F(A,n)=0.$$

If $\left(\frac{d_0}{p}\right)=0,1$ *for every prime* p *with* $2\nmid \operatorname{ord}_p n$, *setting* $n_0=n/m^2$ *and* $H(d/m^2)=\{I_0,A_0,A_0^2\}$ *with* $A_0^3=I_0$ *we then have*

$$F(A,n)=\begin{cases}(-1)^{\mu}\cdot m\prod_{p\mid m}\left(1-\frac{1}{p}\left(\frac{d/m^2}{p}\right)\right)\prod_{\substack{p\in R(I_0)\\ p\nmid d_0}}(1+\operatorname{ord}_p n_0) & \\ \qquad \text{if } q\notin R(A_0) \text{ for every prime } q \text{ with } 3\mid(\operatorname{ord}_q n_0+1), \\ 0 \quad \text{otherwise},\end{cases}$$

where p *runs over all distinct primes and*

$$\mu=\sum_{\substack{p\in R(A_0)\\ \operatorname{ord}_p n_0\equiv 1\ (\mathrm{mod}\ 3)}}1.$$

Moreover, we have

$$R(I,n)=(N(n,d)+2w(d)F(A,n))/3$$

and

$$R(A,n)=(N(n,d)-w(d)F(A,n))/3.$$

Proof. From Remark 3.1 we know that $R(A^2,n)=R(A^{-1},n)=R(A,n)$ and so $N(n,d)=R(I,n)+2R(A,n)$. As $F(A,n)=(R(I,n)-R(A,n))/w(d)$ we then obtain $R(I,n)=(N(n,d)+2w(d)F(A,n))/3$ and $R(A,n)=(N(n,d)-w(d)F(A,n))/3$.

From Theorems 4.1, 8.3 and the above we know that (i) and (ii) hold. Now consider (iii). Suppose $(n,f^2)=m^2$ for $m\in\mathbb{N}$ and $h(d/m^2)=3$. If there is a prime p such that $\left(\frac{d_0}{p}\right)=-1$ and $2\nmid \operatorname{ord}_p n$, then $N(n,d)=0$ and so $R(I,n)=R(A,n)=R(A^2,n)=F(A,n)=0$. Now suppose $\left(\frac{d_0}{p}\right)=0,1$ for every prime p with $2\nmid \operatorname{ord}_p n$. Set $n_0=n/m^2$. Note that $\varphi_{1,m}(A)=A_0$ or A_0^{-1}. By Theorem 8.3 and Remark 7.1 we have

$$F(A,n)=m\prod_{p\mid m}\left(1-\frac{1}{p}\left(\frac{d/m^2}{p}\right)\right)F(A_0,n_0),$$

where p runs over all distinct prime divisors of m. Clearly

$$\frac{d}{m^2}=d_0\left(\frac{f}{m}\right)^2 \quad\text{and}\quad \left(n_0,\left(\frac{f}{m}\right)^2\right)=1.$$

If p is a prime such that $p \mid n_0$, then $p \nmid \frac{f}{m}$ and so $p \nmid f(d/m^2)$. Now applying Theorems 7.4(i) and 8.6(i) we see that

$$F(A_0,n_0) = \prod_{p\mid n_0} F(A_0, p^{\operatorname{ord}_p n_0})$$
$$= \begin{cases} 0 & \text{if there is a prime } q \text{ such that } q \in R(A_0) \text{ and } 3 \mid (\operatorname{ord}_q n_0 + 1), \\ (-1)^\mu \prod\limits_{\substack{p \in R(I_0) \\ p \nmid d_0}} (1+\operatorname{ord}_p n_0) & \text{otherwise}, \end{cases}$$

where p runs over all distinct prime divisors of n_0. Thus (iii) follows and the theorem is proved.

For negative discriminants d it is known (see for example [WH, Proposition, p. 132])

Lemma 10.1. *Let $d < 0$ be a discriminant. Then $h(d) = 3$ if and only if $d = -23, -31, -44, -59, -76, -83, -92, -107, -108, -124, -139, -172, -211, -243, -268, -283, -307, -331, -379, -499, -547, -643, -652, -883, -907$.*

For positive discriminants d we know that $h(d) = 3$ for $d = 148, 229, 257, 404, \ldots$.

Theorem 10.2. *Let $d < 0$ be a discriminant with conductor f. Suppose $h(d) = 3$ and $H(d) = \{I, A, A^2\}$ with $A^3 = I$. Let $n \in \mathbb{N}$ and $F(A,n) = (R(I,n) - R(A,n))/2$.*

(i) *If $(n,f) = 1$, then*

$$F(A,n) = \begin{cases} 0 & \text{if there is a prime } p \text{ such that } \left(\frac{d}{p}\right) = -1 \text{ and } 2 \nmid \operatorname{ord}_p n, \\ 0 & \text{if there is a prime } p \text{ such that } p \in R(A) \text{ and } 3 \mid (1+\operatorname{ord}_p n), \\ (-1)^\mu \prod\limits_{p \nmid d,\, p \in R(I)} (1+\operatorname{ord}_p n) & \text{otherwise}, \end{cases}$$

where in the product p runs over all distinct prime divisors of n and

$$\mu = \sum_{\substack{p \in R(A) \\ \operatorname{ord}_p n \equiv 1 \ (\mathrm{mod}\ 3)}} 1.$$

(ii) *Suppose $(n,f) > 1$ and $d \neq -92, -124$. Then $F(A,n) = 0$.*

(iii) *Suppose $(n,f) > 1$ and $d = -92, -124$. Then $I = [1, 0, -d/4]$ and we may take $A = [3, 2, 8]$ or $[5, 4, 7]$ according as $d = -92$ or -124.*

If $2\,\|\,n$, *then* $F(A,n)=0$. *If* $4\mid n$, *then*

$$F(A,n)=\begin{cases} 0 & \text{if there is a prime } p \text{ such that } \left(\frac{d/4}{p}\right)=-1 \\ & \quad \text{and } 2\nmid \operatorname{ord}_p n, \\ 0 & \text{if there is a prime } p \text{ such that } p\in R\left([2,1,\frac{4-d}{32}]\right) \\ & \quad \text{and } 3\mid \left(1+\operatorname{ord}_p \frac{n}{4}\right), \\ (-1)^{\mu} \displaystyle\prod_{\substack{p\in R([1,1,\frac{4-d}{16}])\\ p\neq -d/4}} \left(1+\operatorname{ord}_p \frac{n}{4}\right) & \text{otherwise,} \end{cases}$$

where in the product p runs over all distinct prime divisors of $n/4$ *and*

$$\mu=\sum_{\substack{p\in R([2,1,\frac{4-d}{32}])\\ \operatorname{ord}_p \frac{n}{4}\equiv 1 \pmod 3}} 1.$$

Proof. Putting $m=1$ in Theorem 10.1(iii) we obtain (i). Now suppose $(n,f)>1$. If (n,f^2) is not a square, then $F(A,n)=0$ by Theorem 10.1. Assume $(n,f^2)=m^2$ for $m\in\mathbb{N}-\{1\}$. If $d\neq -92,-124$, using Lemma 10.1 and (9.3) we see that $h(d/m^2)=1$ and so $F(A,n)=0$ by Theorem 10.1(ii).

If $d=-92,-124$, then $f=2$, $m=2$ and $h(d/m^2)=h(d/4)=3$ by Lemma 10.1. It is easy to see that

$$H\left(\frac{d}{4}\right)=\left\{\left[1,1,\frac{4-d}{16}\right],\ \left[2,1,\frac{4-d}{32}\right],\ \left[2,-1,\frac{4-d}{32}\right]\right\}.$$

Thus applying Theorem 10.1 we obtain (iii). So the theorem is proved.

11. Formulas for $R(K,n)$ ($K\in H(d)$) when $H(d)\cong\mathbb{Z}_4$. For $m\in\mathbb{N}$, throughout this section we let $\mathbb{Z}_m$ be the additive group consisting of residue classes modulo m.

Let $d<0$ be a discriminant. We know that $h(d)=4$ if and only if $-d$ has one of the 84 values listed in [WL, Proposition 1.1]. If $h(d)=4$, then clearly $H(d)\cong\mathbb{Z}_4$ or $H(d)\cong\mathbb{Z}_2\times\mathbb{Z}_2$. Checking the group structure of $H(d)$, we find

Proposition 11.1. *Let $d<0$ be a discriminant such that $h(d)=4$. Then*

(i) $H(d)\cong\mathbb{Z}_4$ *if and only if d has one of the following* 50 *values*:

$-39, -55, -56, -63, -68, -80, -128, -136, -144, -155, -156,$
$-171, -184, -196, -203, -208, -219, -220, -252, -256, -259,$
$-275, -291, -292, -323, -328, -355, -363, -387, -388, -400,$
$-475, -507, -568, -592, -603, -667, -723, -763, -772, -955,$
$-1003, -1027, -1227, -1243, -1387, -1411, -1467, -1507, -1555.$

(ii) $H(d)\cong\mathbb{Z}_2\times\mathbb{Z}_2$ *if and only if* d *has one of the following* 34 *values*:

$-84, -96, -120, -132, -160, -168, -180, -192, -195, -228, -240,$
$-280, -288, -312, -315, -340, -352, -372, -408, -435, -448,$
$-483, -520, -532, -555, -595, -627, -708, -715, -760, -795,$
$-928, -1012, -1435.$

For positive discriminants d we know that $h(d)=4$ for $d=60,96,105,120,136,140,145,156,160,165,168,192,\dots$.

THEOREM 11.1. *Let* d *be a discriminant with conductor* f *and* $d_0=d/f^2$. *Suppose* $H(d)=\{I,A,A^2,A^3\}\cong\mathbb{Z}_4$. *Let* $n\in\mathbb{N}$ *and* $F(A,n)=(R(I,n)-R(A^2,n))/w(d)$.

(i) *If* (n,f^2) *is not a square, then* $F(A,n)=0$.
(ii) *If* $(n,f^2)=m^2$ *with* $m\in\mathbb{N}$ *and* $h(d/m^2)\neq 4$, *then* $F(A,n)=0$.
(iii) *If* $(n,f^2)=m^2$ *with* $m\in\mathbb{N}$ *and* $h(d/m^2)=4$, *setting* $n_0=n/m^2$ *and* $H(d/m^2)=\{I_0,A_0,A_0^2,A_0^3\}$ *with* $A_0^4=I_0$ *we then have*

$$F(A,n)=\prod_{p\notin R(I_0)\cup R(A_0^2)}\frac{1+(-1)^{\operatorname{ord}_p n_0}}{2}\cdot m\prod_{p\mid m}\left(1-\frac{1}{p}\left(\frac{d/m^2}{p}\right)\right)\times(-1)^{\mu}\prod_{\substack{p\in R(I_0)\cup R(A_0^2)\\ p\nmid d_0}}(1+\operatorname{ord}_p n_0),$$

where p *runs over all distinct primes and*

$$\mu=\sum_{\substack{p\in R(A_0)\\ \operatorname{ord}_p n_0\equiv 2\ (\mathrm{mod}\ 4)}}1+\sum_{\substack{p\in R(A_0^2)\\ \operatorname{ord}_p n_0\equiv 1\ (\mathrm{mod}\ 2)}}1.$$

Proof. (i) and (ii) follow from Theorem 8.3. Now suppose $(n,f^2)=m^2$ with $m\in\mathbb{N}$ and $h(d/m^2)=4$. From Theorem 2.1 we know that $\varphi_{1,m}$ is a surjective homomorphism from $H(d)$ to $H(d/m^2)$ and $H(d/m^2)\cong H(d)/\operatorname{Ker}\varphi_{1,m}$. Since $h(d)=h(d/m^2)=4$ we infer that $\operatorname{Ker}\varphi_{1,m}=I$, $H(d/m^2)\cong\mathbb{Z}_4$ and so we may assume $H(d/m^2)=\{I_0,A_0,A_0^2,A_0^3\}$ with $A_0^4=I_0$. Clearly $\varphi_{1,m}(A)=A_0$ or A_0^3 and so $F(\varphi_{1,m}(A),n_0)=F(A_0,n_0)$ by Remark 7.1. Thus applying Theorems 8.3 and 7.4(ii) we have

$$\begin{aligned}F(A,n)&=m\prod_{p\mid m}\left(1-\frac{1}{p}\left(\frac{d/m^2}{p}\right)\right)F(A_0,n_0)\\&=m\prod_{p\mid m}\left(1-\frac{1}{p}\left(\frac{d/m^2}{p}\right)\right)\prod_{p\mid n_0}F(A_0,p^{\operatorname{ord}_p n_0}),\end{aligned}$$

where p runs over all distinct primes. As $d/m^2=d_0(f/m)^2$, $(n_0,(f/m)^2)=1$ and $f(d/m^2)=f/m$ we have $(n_0,f(d/m^2))=1$. Suppose that p is a prime such that $p\,|\,n_0$. Then $p\nmid \frac{f}{m}$. If $p\,|\,d_0$, then $p\in R(I_0)$ by Corollary 8.1(ii). Hence $\left(\frac{d_0}{p}\right)=-1$ or $p\in R(A_0)$ if and only if $p\notin R(I_0)\cup R(A_0^2)$. Now from Theorem 8.7 we see that

$$\begin{aligned}
&\prod_{p|n_0} F(A_0, p^{\operatorname{ord}_p n_0})\\
&= (-1)^{\mu} \prod_{(\frac{d_0}{p})=-1} \frac{1+(-1)^{\operatorname{ord}_p n_0}}{2} \prod_{p\in R(A_0)} \frac{1+(-1)^{\operatorname{ord}_p n_0}}{2}\\
&\quad\times \prod_{\substack{p\in R(I_0)\cup R(A_0^2)\\ p\nmid d_0}} (1+\operatorname{ord}_p n_0)\\
&= (-1)^{\mu} \prod_{p\notin R(I_0)\cup R(A_0^2)} \frac{1+(-1)^{\operatorname{ord}_p n_0}}{2} \prod_{\substack{p\in R(I_0)\cup R(A_0^2)\\ p\nmid d_0}} (1+\operatorname{ord}_p n_0),
\end{aligned}$$

where p runs over all distinct prime divisors of n_0.

By the above, the theorem is proved.

THEOREM 11.2. *Let d be a discriminant with conductor f. Suppose $H(d)=\{I,A,A^2,A^3\}\cong\mathbb{Z}_4$. Let $n\in\mathbb{N}$ and $F(A^2,n)=(R(I,n)-2R(A,n)+R(A^2,n))/w(d)$. Let $N(n,d)$ be as in Theorem* 4.1.

(i) *If (n,f^2) is not a square, then $F(A^2,n)=0$.*

(ii) *If $(n,f^2)=m^2$ with $m\in\mathbb{N}$ and $h(d/m^2)=1$ (i.e. $t(d/m^2)=0$), then $F(A^2,n)=0$.*

(iii) *If $(n,f^2)=m^2$ with $m\in\mathbb{N}$ and $h(d/m^2)>1$ (i.e. $t(d/m^2)=1$), then*

$$F(A^2,n)=(-1)^{\sum_{p\in R(A_0)}\operatorname{ord}_p n}\cdot\frac{N(n,d)}{w(d)},$$

where A_0 is a generator of $H(d/m^2)$ and p runs over all distinct primes satisfying $p\,|\,n$ and $p\in R(A_0)$.

Proof. Clearly (i) and (ii) follow from Theorem 8.3 and Lemma 9.1. Now suppose $(n,f^2)=m^2$ with $m\in\mathbb{N}$ and $h(d/m^2)>1$. By Theorem 2.1 we have $H(d/m^2)\cong H(d)/\operatorname{Ker}\varphi_{1,m}$. Thus $H(d/m^2)\cong\mathbb{Z}_2$ or $H(d/m^2)\cong\mathbb{Z}_4$. Let I_0 be the principal class in $H(d/m^2)$ and let A_0 be a generator of $H(d/m^2)$. By Theorem 2.1 we have $\varphi_{1,m}(A)=A_0$ or A_0^{-1}. Set $d_0=d/f^2$, $h_0=h(d/m^2)$ and $n_0=n/m^2$. Using Theorem 8.3 we see that

$$F(A^2,n)=m\prod_{p|m}\left(1-\frac{1}{p}\left(\frac{d/m^2}{p}\right)\right)F(A_0^{h_0/2},n_0),$$

where p runs over all distinct prime divisors of m. As $d/m^2 = d_0(f/m)^2$ and so $(n_0, f(d/m^2)) = 1$, from Theorems 7.4, 8.5(i) and 8.7 we see that

$$\begin{aligned} &F(A_0^{h_0/2}, n_0)\\ &= \prod_{p\mid n_0} F(A_0^{h_0/2}, p^{\mathrm{ord}_p n_0})\\ &= \prod_{(\frac{d_0}{p})=-1} \frac{1+(-1)^{\mathrm{ord}_p n_0}}{2} \cdot (-1)^{\sum_{p\in R(A_0)} \mathrm{ord}_p n_0} \prod_{(\frac{d_0}{p})=1} (1+\mathrm{ord}_p n_0), \end{aligned}$$

where p runs over all distinct prime divisors of n_0. Now combining the above with Theorem 4.1 and Lemma 9.1 we obtain (iii). This completes the proof of the theorem.

THEOREM 11.3. *Let d be a discriminant with conductor f and $d_0 = d/f^2$. Suppose $H(d) = \{I, A, A^2, A^3\} \cong \mathbb{Z}_4$ and $n \in \mathbb{N}$. Then*

$$\begin{aligned} R(I,n) &= (F(I,n) + 2F(A,n) + F(A^2,n))w(d)/4,\\ R(A,n) = R(A^3,n) &= (F(I,n) - F(A^2,n))w(d)/4, \qquad (11.1)\\ R(A^2,n) &= (F(I,n) - 2F(A,n) + F(A^2,n))w(d)/4, \end{aligned}$$

where $F(I,n), F(A,n)$ and $F(A^2,n)$ are given by Remark 7.1, *Theorems* 11.1 *and* 11.2 *respectively.*

Proof. Let $F(A,n)$ and $F(A^2,n)$ be given as in Theorem 7.4. From Theorem 7.3 we have

$$R(A^k,n) = \frac{w(d)}{4}\Big(F(I,n) + 2\cos\frac{2\pi k}{4}\, F(A,n) + (-1)^k F(A^2,n)\Big)$$

for $k \in \mathbb{Z}$. Thus (11.1) holds. Now applying Remark 7.1, Theorems 11.1 and 11.2 yields the result.

References

[B] D. A. Buell, *Binary Quadratic Forms*, Springer, New York, 1989.

[C] H. Cohen, *A Course in Computational Algebraic Number Theory*, Grad. Texts in Math. 138, Springer, Berlin, 1993.

[Coh] H. Cohn, *Advanced Number Theory*, Dover, New York, 1980.

[Cox] D. A. Cox, *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*, Wiley, New York, 1989.

[D] P. G. L. Dirichlet, *Lectures on Number Theory* (Supplements by R. Dedekind), transl. by J. Stillwell, Amer. Math. Soc., 1999, pp. 217–221.

[H] L. K. Hua, *Introduction to Number Theory*, Springer, Berlin, 1982, pp. 279–283, 307–308, 321–322.

[HKW] J. G. Huard, P. Kaplan and K. S. Williams, *The Chowla–Selberg formula for genera*, Acta Arith. 73 (1995), 271–301.

[KW1] P. Kaplan and K. S. Williams, *On a formula of Dirichlet*, Far East J. Math. Sci. 5 (1997), 153–157.

[KW2] —, —, *The genera representing a positive integer*, Acta Arith. 102 (2002), 353–361.

[KW3] —, —, *On the number of representations of a positive integer by a binary quadratic form*, ibid. 114 (2004), 87–98.

[MOS] W. Magnus, F. Oberhettinger and R. P. Soni, *Formulas and Theorems for the Special Functions of Mathematical Physics*, 3rd ed., Springer, New York, 1966, pp. 256–259.

[MW1] H. Muzaffar and K. S. Williams, *A restricted Epstein zeta function and the evaluation of some definite integrals*, Acta Arith. 104 (2002), 23–66.

[MW2] —, —, *Evaluation of Weber's functions at quadratic irrationalities*, JP J. Algebra Number Theory Appl. 4 (2004), 209–259.

[NZM] I. Niven, H. S. Zuckerman and H. L. Montgomery, *An Introduction to the Theory of Numbers*, 5th ed., Wiley, New York, 1991.

[S] Z. H. Sun, *Quartic residues and binary quadratic forms*, J. Number Theory 113 (2005), 10–52.

[WH] K. S. Williams and R. H. Hudson, *Representation of primes by the principal form of discriminant* $-D$ *when the class number* $h(-D)$ *is* 3, Acta Arith. 57 (1991), 131–153.

[WL] K. S. Williams and D. Liu, *Representation of primes by the principal form of negative discriminant* Δ *when* $h(\Delta)$ *is* 4, Tamkang J. Math. 25 (1994), 321–334.

Department of Mathematics
Huaiyin Teachers College
Huaian, Jiangsu 223001, P.R. China
E-mail: hyzhsun@public.hy.js.cn
http://www.hytc.cn/xsjl/szh

Centre for Research in Algebra and Number Theory
School of Mathematics and Statistics
Carleton University
Ottawa, Ontario K1S 5B6, Canada
E-mail: williams@math.carleton.ca
http://mathstat.carleton.ca/˜williams

Received on 3.12.2004
and in revised form on 24.12.2005 (4899)