ACTA ARITHMETICA
114.1 (2004)

On the number of representations of a positive integer by a binary quadratic form

by

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

0. Notation. Throughout this paper n denotes a positive integer and d denotes a *discriminant*, that is, d is a nonsquare integer such that $d \equiv 0$ or $1 \pmod 4$. We set

$$w(d) = \begin{cases} 6 & \text{if } d = -3, \\ 4 & \text{if } d = -4, \\ 2 & \text{if } d < -4, \\ 1 & \text{if } d > 0. \end{cases} \tag{0.1}$$

If $d > 0$ we let

$$\varepsilon(d) = \frac{1}{2}\,(x_0 + y_0\sqrt{d}), \tag{0.2}$$

where (x_0, y_0) is the solution of $x^2 - dy^2 = 4$ in positive integers with y least. If m is a positive integer such that $m^2 \mid d$ and d/m^2 is a discriminant, we set

$$\lambda(d,m) = \begin{cases} 1 & \text{if } d < 0, \\ \dfrac{\log \varepsilon(d)}{\log \varepsilon(d/m^2)} & \text{if } d > 0. \end{cases} \tag{0.3}$$

The *conductor* $f = f(d)$ of the discriminant d is the largest positive integer f such that d/f^2 is a discriminant. The discriminant $\Delta = \Delta(d) = d/f(d)^2$ is called the *fundamental discriminant* associated with d. If $f(d) = 1$, then d is called *fundamental*. We denote by $M = M(n,d)$ the largest positive integer M such that $M^2 \mid n$ and $M \mid f$. Equivalently M is the largest positive integer such that $M^2 \mid n$, $M^2 \mid d$ and d/M^2 is a discriminant.

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

Key words and phrases: representations of an integer by a binary quadratic form.

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

Let $(a,b,c)=ax^2+bxy+cy^2$ be a primitive, integral, binary quadratic form of discriminant d, which is irreducible in $\mathbb{Z}[x,y]$, so that a, b, c are integers such that $\gcd(a,b,c)=1$ and $d=b^2-4ac\equiv 0$ or $1 \pmod 4$ is not a square in $\mathbb{Z}$. If $d<0$ we only consider positive-definite forms, that is, forms (a,b,c) with $a>0$. The positive integer n is said to be *represented* by the form (a,b,c) if there exists $(x,y)\in\mathbb{Z}\times\mathbb{Z}$ such that $n=ax^2+bxy+cy^2$. In the case $d<0$ every representation (x,y) of n by (a,b,c) is said to be *primary*. In the case $d>0$ only those representations (x,y) of n by (a,b,c) are called *primary* that satisfy the inequalities

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

The number of primary representations of n by the form (a,b,c) is denoted by $R_{(a,b,c)}(n,d)$. It is known that $R_{(a,b,c)}(n,d)$ is finite. The *class* of the form (a,b,c) is the set $[a,b,c]$ given by

$$\begin{aligned}[a,b,c]=\{a(px+qy)^2+b(px+qy)(rx+sy)+c(rx+sy)^2 \mid \\ p,q,r,s\in\mathbb{Z},\ ps-qr=1\}.\end{aligned}$$

The set of distinct classes of primitive, integral, binary quadratic forms of discriminant d is denoted by $H(d)$. Let $K\in H(d)$. If $[a,b,c]=[a',b',c']=K$ then $R_{(a,b,c)}(n,d)=R_{(a',b',c')}(n,d)$ so we can define

$$R_K(n,d)=R_{(a,b,c)}(n,d) \quad \text{for any } (a,b,c)\in K.$$

With respect to Gaussian composition (see for example [2, Chapter 4]), $H(d)$ is a finite abelian group called the *form class group*. The order of $H(d)$ is called the *form class number* and is denoted by $h(d)$. The *genus group* of $H(d)$ is the quotient group $G(d)=H(d)/H^2(d)$. It is known that $|G(d)|=2^{t(d)}$, where $t(d)$ is the nonnegative integer given by

$$(0.4) \qquad t(d)=\begin{cases}\omega(d)-2 & \text{if } d\equiv 4 \pmod{16},\\ \omega(d) & \text{if } d\equiv 0 \pmod{32},\\ \omega(d)-1 & \text{otherwise,}\end{cases}$$

where $\omega(d)$ is the number of distinct prime factors of d. The number of form classes in each genus $G\in G(d)$ is $h(d)/2^{t(d)}$. For $G\in G(d)$ we set

$$(0.5) \qquad R_G(n,d)=\sum_{K\in G}R_K(n,d).$$

An *odd prime discriminant* is a discriminant of the form $p^*=(-1)^{(p-1)/2}p$, where p is an odd prime. The discriminants -4, 8, -8 are called *even prime discriminants*. Set $t=t(d)$, where $t(d)$ is defined in (0.4). The prime discriminants corresponding to the discriminant d are the discriminants

$p_1^*, \dots, p_{t+1}^*$, together with p_{t+2}^* if $d \equiv 0 \pmod{32}$, where $p_1, \dots, p_{t+1}$ are given as follows:

(i) $d \equiv 1 \pmod 4$ or $d \equiv 4 \pmod{16}$
$p_1 < \dots < p_{t+1}$ are the odd prime divisors of d.

(ii) $d \equiv 12 \pmod{16}$ or $d \equiv 16 \pmod{32}$
$p_1 < \dots < p_t$ are the odd prime divisors of d and $p_{t+1}^* = -4$.

(iii) $d \equiv 8 \pmod{32}$
$p_1 < \dots < p_t$ are the odd prime divisors of d and $p_{t+1}^* = 8$.

(iv) $d \equiv 24 \pmod{32}$
$p_1 < \dots < p_t$ are the odd prime divisors of d and $p_{t+1}^* = -8$.

(v) $d \equiv 0 \pmod{32}$
$p_1 < \dots < p_{t-1}$ are the odd prime divisors of d, $p_t^* = -4$, $p_{t+1}^* = 8$, and $p_{t+2}^* = -8$.

The set of prime discriminants corresponding to d is denoted by $P(d)$. We note that these are coprime in pairs if $d \not\equiv 0 \pmod{32}$. The set of all products of pairwise coprime elements of $P(d)$ is denoted by $F(d)$. The empty product 1 is included in $F(d)$. Thus, for example, with $d = 384 = 2^7 \cdot 3$, we have

$$t(d) = 2, \quad p_1 = 3, \quad p_1^* = -3, \quad p_2^* = -4, \quad p_3^* = 8, \quad p_4^* = -8,$$

and

$$P(d) = \{-3, -4, 8, -8\}, \quad F(d) = \{1, -3, -4, 8, -8, 12, -24, 24\}.$$

Properties of the sets $P(d)$ and $F(d)$ are given in [4, Lemma 2.1, p. 277] and [9, Lemma 1, p. 29].

Let $p^* \in P(d)$ and $K \in H(d)$. For any positive integer k which is coprime with p^* and represented by K, it is known that $\left(\frac{p^*}{k}\right)$ has the same value so we can set

$$\gamma_{p^*}(K) = \left(\frac{p^*}{k}\right) = \pm 1.$$

A main result of Gauss's theory of genera is that the genera are the sets of classes in $H(d)$ giving the same value to γ_{p^*} for each $p^* \in P(d)$. Thus, for each genus $G \in G(d)$ and each $p^* \in P(d)$, we can set $\gamma_{p^*}(G) = \gamma_{p^*}(K)$, where K is any class in G. The definition of $\gamma_{p^*}(G)$ ($p^* \in P(d)$) is extended to $\gamma_{d_1}(G)$ ($d_1 \in F(d)$) by

$$\gamma_{d_1}(G) = \prod_{p^* \in P(d_1)} \gamma_{p^*}(G) = \left(\frac{d_1}{a}\right) = \pm 1, \tag{0.6}$$

where the class $[a, b, c] \in G$ is chosen so that a is prime to d.

A prime p is said to be a *null prime* with respect to n and d if

$$v_p(n) \equiv 1 \pmod 2, \quad v_p(n) < 2v_p(f), \tag{0.7}$$

where $p^{v_p(k)}$ is the largest power of p dividing the positive integer k. The set of all such null primes is denoted by $\mathrm{Null}(n,d)$. The following elementary result is proved in [4, Proposition 4.1] for $d<0$ and for both positive and negative d in [9, Lemma 5].

PROPOSITION 1. *If* $\mathrm{Null}(n,d)\neq\emptyset$ *then* $R_K(n,d)=0$ *for each* $K\in H(d)$.

The following result is proved in [4, Theorem 8.1, p. 289] in the case $d<0$ and in [9, Theorem 1, p. 38] in the case $d>0$.

PROPOSITION 2. *Let* $G\in G(d)$. *If* $\mathrm{Null}(n,d)=\emptyset$ *then*

$$R_G(n,d)=\lambda(d,M)\,\frac{h(d)}{h(d/M^2)}\,\frac{w(d/M^2)}{2^{t(d)+1}}\times\sum_{d_1\in F(d/M^2)}\gamma_{d_1}(G)\sum_{\mu\nu=n/M^2}\left(\frac{d_1}{\mu}\right)\left(\frac{d/M^2d_1}{\nu}\right).$$

If $\mathrm{Null}(n,d)\neq\emptyset$ *then* $R_G(n,d)=0$.

The proof of Proposition 2 follows from Gauss's theory of genera and so is an elementary theorem.

1. Introduction. From Proposition 2 it is possible to give a formula for $R_{(a,b,c)}(n,d)$ when $[a,b,c]$ belongs to a genus consisting of exactly one class or consisting of exactly two classes K and K^{-1} with $K\neq K^{-1}$. A formula for $R_{(a,b,c)}(n,d)$ when $[a,b,c]$ belongs to a genus consisting of exactly one class has been given by Hall [3]. No formula is known for $R_{(a,b,c)}(n,d)$ for an arbitrary form (a,b,c). However, a number of authors (for example van der Blij [1], Lomadze [6]–[8], Vepkhvadze [10]–[14]) have obtained formulae for $R_{(a,b,c)}(n,d)$ for certain special forms $ax^2+bxy+cy^2$, which belong to genera having at least three classes or consisting of exactly two classes K_1 and K_2 with $K_1\neq K_2$, $K_1=K_1^{-1}$, $K_2=K_2^{-1}$. In most cases their formulae for $R_{(a,b,c)}(n,d)$ have d nonfundamental and depend upon the coefficients in the expansion of certain products of theta functions. For example Lomadze [7, Theorem 7a] proved

$$R_{(1,0,32)}(n,-128)=\begin{cases}\displaystyle\sum_{d\mid n}\left(\frac{-2}{d}\right)+\frac{1}{2}\,v(n) & \text{if } \alpha=0,\ u\equiv 1 \pmod 8,\\[2ex] \displaystyle 2\sum_{d\mid n}\left(\frac{-2}{d}\right) & \begin{array}{l}\text{if } \alpha=2,\ u\equiv 1 \pmod 8,\\ \text{or } \alpha>3,\ u\equiv 1 \text{ or } 3 \pmod 8,\end{array}\\[2ex] 0 & \text{otherwise,}\end{cases}$$

where $n=2^\alpha u$, u odd, and $v(n)$ denotes the coefficient of Q^n in the expansion of the function $\theta_{80}(\tau;0,8)\theta_{01}(\tau;0,16)$ in powers of $Q=\exp(2\pi i\tau)$, where

$$\theta_{gh}(\tau; c, N) = \sum_{\substack{m=-\infty \\ m \equiv c \pmod N}}^{\infty} (-1)^{h(m-c)/N} Q^{(m+g/2)^2/2N}.$$

We note that the second and third lines of the formulae for $R_{(1,0,32)}(n, -128)$ do not depend upon the quantity $v(n)$. They depend at most on the values of the Kronecker symbol $\left(\frac{-2}{d}\right)$ for $d \mid n$ and thus are elementary formulae even though they were derived by advanced analytical techniques. In this paper we prove a general theorem by entirely elementary means from which these and other elementary formulae follow as special cases.

2. Statement and proof of main result

THEOREM 1. *Let d be a discriminant for which there exists a positive integer m such that d/m^2 is a discriminant and either*

(2.1) $$H(d/m^2) = \mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2 \qquad \text{(Case I)}$$

or

(2.2) $$H(d/m^2) = \mathbb{Z}_4 \times \mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2 \qquad \text{(Case II)}.$$

Let $K = [a, b, c] \in H(d)$ with a, b, c chosen so that

(2.3) $$(a, d) = 1, \qquad m \mid b, \qquad m^2 \mid c.$$

Let n be a positive integer. If $\mathrm{Null}(n, d) \neq \emptyset$ *then $R_K(n, d) = 0$. If* $\mathrm{Null}(n, d) = \emptyset$ *and $m^2 \mid n$ then in Case* I

$$R_K(n, d) = \lambda(d, M) \frac{w(d/M^2)}{2^{t(d/m^2)+1}} \frac{h(d/m^2)}{h(d/M^2)} \times \sum_{d_1 \in F(d/M^2)} \left(\frac{d_1}{a}\right) \sum_{\mu\nu = n/M^2} \left(\frac{d_1}{\mu}\right) \left(\frac{d/M^2 d_1}{\nu}\right)$$

and in Case II

$$R_K(n, d) = \lambda(d, M) \frac{w(d/M^2)}{2^{t(d/m^2)+2}} \frac{h(d/m^2)}{h(d/M^2)} \times \sum_{d_1 \in F(d/M^2)} \left(\frac{d_1}{a}\right) \sum_{\mu\nu = n/M^2} \left(\frac{d_1}{\mu}\right) \left(\frac{d/M^2 d_1}{\nu}\right)$$

provided $[a, b/m, c/m^2] \neq [a, b/m, c/m^2]^{-1}$.

Proof. If $\mathrm{Null}(n, d) \neq \emptyset$ then, by Proposition 1, we have $R_K(n, d) = 0$. Hence we may suppose that $\mathrm{Null}(n, d) = \emptyset$. Let m be a positive integer such that d/m^2 is a discriminant and $m^2 \mid n$. By (0.7) we have

(2.4) $$\mathrm{Null}(n/m^2, d/m^2) = \emptyset.$$

As m is a positive integer such that $m^2 \mid n$, $m^2 \mid d$ and d/m^2 is a discriminant then $m \mid M = M(n,d)$ and

$$M(n/m^2, d/m^2) = \frac{M(n,d)}{m}. \tag{2.5}$$

Hence

$$\frac{d/m^2}{M(n/m^2, d/m^2)^2} = \frac{d/m^2}{(M(n,d)/m)^2} = \frac{d}{M(n,d)^2} = \frac{d}{M^2}, \tag{2.6}$$

$$\frac{n/m^2}{M(n/m^2, d/m^2)^2} = \frac{n/m^2}{(M(n,d)/m)^2} = \frac{n}{M(n,d)^2} = \frac{n}{M^2}. \tag{2.7}$$

Applying [4, Lemma 6.2, p. 286] in the case $d < 0$ and [9, Lemma 14, p. 35] in the case $d > 0$ to each prime dividing m, we obtain

$$R_K(n,d) = \lambda(d,m) R_{[a,b/m,c/m^2]}(n/m^2, d/m^2). \tag{2.8}$$

Let $G \in G(d/m^2)$ be the genus to which the class $[a, b/m, c/m^2]$ belongs. By (2.4)–(2.7) and Proposition 2, we obtain

$$\begin{aligned} R_G(n/m^2, d/m^2) &= \lambda(d/m^2, M/m) \frac{w(d/M^2)}{2^{t(d/m^2)+1}} \frac{h(d/m^2)}{h(d/M^2)} \\ &\quad \times \sum_{d_1 \in F(d/M^2)} \gamma_{d_1}(G) \sum_{\mu\nu = n/M^2} \left(\frac{d_1}{\mu}\right)\left(\frac{d/M^2 d_1}{\nu}\right). \end{aligned} \tag{2.9}$$

Now from (0.3) we deduce

$$\lambda(d,m)\lambda(d/m^2, M/m) = \lambda(d,M) \tag{2.10}$$

so that by (0.6) the equation (2.9) becomes

$$\begin{aligned} R_G(n/m^2, d/m^2) &= \frac{\lambda(d,M)}{\lambda(d,m)} \frac{w(d/M^2)}{2^{t(d/m^2)+1}} \frac{h(d/m^2)}{h(d/M^2)} \\ &\quad \times \sum_{d_1 \in F(d/M^2)} \left(\frac{d_1}{a}\right) \sum_{\mu\nu = n/M^2} \left(\frac{d_1}{\mu}\right)\left(\frac{d/M^2 d_1}{\nu}\right). \end{aligned} \tag{2.11}$$

We now assume that either Case I or Case II holds.

Case I. As $H(d/m^2) = \mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2$ we have $G = \{[a, b/m, c/m^2]\}$. The asserted formula follows from (2.8) and (2.11).

Case II. As $H(d/m^2) = \mathbb{Z}_4 \times \mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2$ and since $[a, b/m, c/m^2] \neq [a, b/m, c/m^2]^{-1}$ we have

$$G = \{[a, b/m, c/m^2], [a, -b/m, c/m^2]\}.$$

Hence

$$\begin{aligned} R_G(n/m^2, d/m^2) &= R_{[a,b/m,c/m^2]}(n/m^2, d/m^2) \\ &\quad + R_{[a,-b/m,c/m^2]}(n/m^2, d/m^2). \end{aligned}$$

Clearly

$$R_{[a,b/m,c/m^2]}(n/m^2, d/m^2) = R_{[a,-b/m,c/m^2]}(n/m^2, d/m^2)$$

so that

$$R_{[a,b/m,c/m^2]}(n/m^2, d/m^2) = \frac{1}{2} R_G(n/m^2, d/m^2). \tag{2.12}$$

The asserted formula now follows from (2.8), (2.11) and (2.12). ∎

We note that when $\mathrm{Null}(n,d) = \emptyset$ and $m^2 \mid n$, the formula for $R_{[a,b,c]}(n,d)$ depends only upon n, d and the genus to which $[a, b/m, c/m^2]$ belongs. In this connection see [15].

3. Some special cases of Theorem 1. The values of d with $-140 \le d < 0$ to which the theorem applies are listed in Table 1.

Table 1

d	$H(d)$	m	d/m^2	$H(d/m^2)$	Corollary	Reference
-44	$\mathbb{Z}_3$	2	-11	$\mathbb{Z}_1$	1	[7, Theorem 1a]
-63	$\mathbb{Z}_4$	3	-7	$\mathbb{Z}_1$	2	
-76	$\mathbb{Z}_3$	2	-19	$\mathbb{Z}_1$	3	[7, Theorem 5a]
-80	$\mathbb{Z}_4$	2	-20	$\mathbb{Z}_2$	4	[7, Theorems 3a, 4a]
-108	$\mathbb{Z}_3$	2	-27	$\mathbb{Z}_1$	5	
-108	$\mathbb{Z}_3$	3	-12	$\mathbb{Z}_1$		
-108	$\mathbb{Z}_3$	6	-3	$\mathbb{Z}_1$		
-128	$\mathbb{Z}_4$	2	-32	$\mathbb{Z}_2$	6	[7, Theorem 7a]
-128	$\mathbb{Z}_4$	4	-8	$\mathbb{Z}_1$		
-135	$\mathbb{Z}_6$	3	-15	$\mathbb{Z}_2$	7	
-140	$\mathbb{Z}_6$	2	-35	$\mathbb{Z}_2$	8	

Applying the theorem to the discriminants in the table, we obtain the following corollaries. The value of $R_K(n,d)$ is only given for those $K \in H(d)$ such that $K = K^{-1}$ and K belongs to a genus containing exactly two classes or K belongs to a genus having three or more classes.

Corollary 1. *Let $n = 2^\alpha 11^\beta N$, where $(N, 22) = 1$. Then, for $\alpha \ge 1$, we have*

$$\begin{aligned} R_{[1,0,11]}(n,-44) &= R_{[3,\pm 2,4]}(n,-44) \\ &= \frac{1}{2}(1+(-1)^\alpha)\left(1+\left(\frac{N}{11}\right)\right)\sum_{d\mid N}\left(\frac{d}{11}\right). \end{aligned}$$

Corollary 2. *Let* $n = 3^\alpha 7^\beta N$, *where* $(N,21) = 1$. *Then, for* $\alpha \geq 1$, *we have*

$$\begin{aligned} R_{[1,1,16]}(n,-63) &= R_{[4,1,4]}(n,-63) \\ &= \frac{1}{2}\left(1+(-1)^\alpha\right)\left(1+\left(\frac{N}{7}\right)\right)\sum_{d\mid N}\left(\frac{d}{7}\right). \end{aligned}$$

Corollary 3. *Let* $n = 2^\alpha 19^\beta N$, *where* $(N,38) = 1$. *Then, for* $\alpha \geq 1$, *we have*

$$\begin{aligned} R_{[1,0,19]}(n,-76) &= R_{[4,\pm 2,5]}(n,-76) \\ &= \frac{1}{2}\left(1+(-1)^\alpha\right)\left(1+\left(\frac{N}{19}\right)\right)\sum_{d\mid N}\left(\frac{d}{19}\right). \end{aligned}$$

Corollary 4. *Let* $n = 2^\alpha 5^\beta N$, *where* $(N,10) = 1$. *Then, for* $\alpha \geq 1$, *we have*

$$\begin{aligned} &R_{[1,0,20]}(n,-80) = R_{[4,0,5]}(n,-80) \\ &\quad = \begin{cases} \dfrac{1}{2}\left(1+(-1)^\alpha\left(\dfrac{-1}{N}\right)\right)\left(1+\left(\dfrac{-5}{N}\right)\right)\displaystyle\sum_{d\mid N}\left(\frac{d}{5}\right) & \textit{if } \alpha \geq 2, \\ 0 & \textit{if } \alpha = 1. \end{cases} \end{aligned}$$

Corollary 5. *Let* $n = 2^\alpha 3^\beta N$, *where* $(N,6) = 1$. *Then, for* $(\alpha,\beta) \neq (0,0)$, *we have*

$$\begin{aligned} R_{[1,0,27]}(n,-108) &= R_{[4,\pm 2,7]}(n,-108) \\ &= \frac{\theta}{2}\left(1+(-1)^\alpha\right)\left(1+\left(\frac{N}{3}\right)\right)\sum_{d\mid N}\left(\frac{d}{3}\right), \end{aligned}$$

where

$$\theta = \begin{cases} 0 & \textit{if } \alpha = 1 \textit{ or } \beta = 1, \\ 1 & \textit{if } \alpha = 0,\ \beta \geq 2 \textit{ or } \alpha \geq 2,\ \beta = 0, \\ 3 & \textit{if } \alpha \geq 2 \textit{ and } \beta \geq 2. \end{cases}$$

Corollary 6. *Let* $n = 2^\alpha N$, *where* $(N,2) = 1$. *Then, for* $\alpha \geq 1$, *we have*

$$\begin{aligned} &R_{[1,0,32]}(n,-128) = R_{[4,4,9]}(n,-128) \\ &\quad = \begin{cases} \left(1+\left(\dfrac{-2}{N}\right)\right)\displaystyle\sum_{d\mid N}\left(\frac{-2}{d}\right) & \textit{if } \alpha \geq 4, \\ \dfrac{1}{2}\left(1+\left(\dfrac{-1}{N}\right)\right)\left(1+\left(\dfrac{-2}{N}\right)\right)\displaystyle\sum_{d\mid N}\left(\frac{-2}{d}\right) & \textit{if } \alpha = 2, \\ 0 & \textit{if } \alpha = 1 \textit{ or } 3. \end{cases} \end{aligned}$$

COROLLARY 7. *Let $n = 3^\alpha 5^\beta N$, where $(N, 15) = 1$. Then, for $\alpha \geq 1$, we have*

$$R_{[1,1,34]}(n,-135) = R_{[4,\pm 3,9]}(n,-135)$$
$$= \begin{cases} \frac{1}{2}\left(1+(-1)^{\alpha+\beta}\left(\frac{N}{5}\right)\right)\left(1+\left(\frac{N}{15}\right)\right)\sum_{d\mid N}\left(\frac{d}{15}\right) & \textit{if } \alpha \geq 2, \\ 0 & \textit{if } \alpha = 1, \end{cases}$$

$$R_{[2,\pm 1,17]}(n,-135) = R_{[5,5,8]}(n,-135)$$
$$= \begin{cases} \frac{1}{2}\left(1-(-1)^{\alpha+\beta}\left(\frac{N}{5}\right)\right)\left(1+\left(\frac{N}{15}\right)\right)\sum_{d\mid N}\left(\frac{d}{15}\right) & \textit{if } \alpha \geq 2, \\ 0 & \textit{if } \alpha = 1. \end{cases}$$

COROLLARY 8. *Let $n = 2^\alpha 5^\beta 7^\gamma N$, where $(N, 70) = 1$. Then, for $\alpha \geq 1$, we have*

$$R_{[1,0,35]}(n,-140) = R_{[4,\pm 2,9]}(n,-140)$$
$$= \frac{1}{4}\left(1+(-1)^{\alpha}\right)\left(1+(-1)^{\beta+\gamma}\left(\frac{N}{7}\right)\right)\left(1+\left(\frac{N}{35}\right)\right)\sum_{d\mid N}\left(\frac{d}{35}\right),$$

$$R_{[3,\pm 2,12]}(n,-140) = R_{[5,0,7]}(n,-140)$$
$$= \frac{1}{4}\left(1+(-1)^{\alpha}\right)\left(1-(-1)^{\beta+\gamma}\left(\frac{N}{7}\right)\right)\left(1+\left(\frac{N}{35}\right)\right)\sum_{d\mid N}\left(\frac{d}{35}\right).$$

Vepkhvadze [16] gave formulae for $R_{[1,0,19]}(n,-76)$ and $R_{[4,\pm 2,5]}(n,-76)$. When $\alpha \geq 1$ his formulae agree with those of Corollary 3. However when $\alpha = 0$ his formulae are not correct, as was noted by Zhuravlev [17] in his review of Vepkhvadze's paper. We correct and extend Vepkhvadze's formulae in the next theorem.

VEPKHVADZE'S THEOREM (corrected and extended). *Let $m \in \{11, 19, 27, 43, 67, 163\}$. Let p denote the unique prime dividing m. Let $m^* = \frac{1}{4}(m+1)$. Let $n = p^\beta N$, where $(N, 2p) = 1$. Then*

$$R_{[1,0,m]}(n,-4m) = -\sum_{x_1^2+x_1x_2+m^*x_2^2=n}(-1)^{x_1},$$

$$R_{[4,\pm 2,m^*]}(n,-4m) = \sum_{d\mid N}\left(\frac{-p}{d}\right) + \frac{1}{2}\sum_{x_1^2+x_1x_2+m^*x_2^2=n}(-1)^{x_1}.$$

Proof. First we note that

$$R_{[4,2,m^*]}(n,-4m) = \sum_{4x_1^2+2x_1x_2+m^*x_2^2=n} 1 = \frac{1}{2}\sum_{x_1^2+x_1x_2+m^*x_2^2=n}\left(1+(-1)^{x_1}\right)$$

$$= \frac{1}{2} R_{[1,1,m^*]}(n,-m) + \frac{1}{2} \sum_{x_1^2+x_1x_2+m^*x_2^2=n} (-1)^{x_1}.$$

As $H(-m)$ consists of the single class $[1,1,m^*]$, by Dirichlet's theorem [4], [5] we have

$$R_{[1,1,m^*]}(n,-m) = 2\sum_{d|n}\left(\frac{-p}{d}\right) = 2\sum_{d|N}\left(\frac{-p}{d}\right).$$

Thus

$$R_{[4,2,m^*]}(n,-4m) = \sum_{d|N}\left(\frac{-p}{d}\right) + \frac{1}{2} \sum_{x_1^2+x_1x_2+m^*x_2^2=n} (-1)^{x_1}.$$

As $[1,0,m]$, $[4,2,m^*]$ and $[4,-2,m^*]$ comprise the three classes of $H(-4m)$, and n is coprime with the conductor of the discriminant $-4m$, namely 2 if $m \neq 27$ and 6 if $m = 27$, by Dirichlet's formula we have

$$\begin{aligned} R_{[1,0,m]}(n,-4m) + R_{[4,2,m^*]}(n,-4m) + R_{[4,-2,m^*]}(n,-4m) \\ = 2\sum_{d|n}\left(\frac{-4m}{d}\right) = 2\sum_{d|N}\left(\frac{-p}{d}\right). \end{aligned}$$

Clearly

$$R_{[4,2,m^*]}(n,-4m) = R_{[4,-2,m^*]}(n,-4m)$$

so that

$$\begin{aligned} R_{[1,0,m]}(n,-4m) &= 2\sum_{d|N}\left(\frac{-p}{d}\right) - 2R_{[4,2,m^*]}(n,-4m) \\ &= 2\sum_{d|N}\left(\frac{-p}{d}\right) - 2\Bigg(\sum_{d|N}\left(\frac{-p}{d}\right) + \frac{1}{2} \sum_{x_1^2+x_1x_2+m^*x_2^2=n} (-1)^{x_1}\Bigg) \\ &= - \sum_{x_1^2+x_1x_2+m^*x_2^2=n} (-1)^{x_1}, \end{aligned}$$

completing the proof. ∎

4. Concluding remarks. The following result is part of [7, Theorem 2a]. It does not follow from Theorem 1.

COROLLARY 9. *Let* $n = 2^\alpha 17^\beta N$, *where* $(N,34) = 1$. *Then*

$$R_{[1,0,17]}(n,-68) = 0 \quad \text{if } N \equiv 3 \pmod 4.$$

This result is the special case $a = 1$, $b = 0$, $c = 17$, $d = -68$ of the following elementary result.

THEOREM 2. *Let* $n = 2^\alpha N$, *where* $(N,2) = 1$. *Let* $K = [a,b,c] \in H(d)$. *If*

$$a \equiv c \equiv 1 \pmod 2, \quad a - c \equiv b \equiv 0 \pmod 4, \quad a - b - c \equiv 0 \pmod 8,$$

then

$$R_K(n,d) = 0 \quad \text{if } N \equiv a + 2 \pmod 4.$$

Proof. Suppose that there exist integers x and y such that

$$n = ax^2 + bxy + cy^2. \tag{4.1}$$

If $4 \mid n$ then

$$x^2 + y^2 \equiv a^2(x^2+y^2) \equiv a(ax^2+bxy+cy^2) = an \equiv 0 \pmod 4$$

so that $x \equiv y \equiv 0$ (mod 2). Hence, dividing out powers of 4 in n, we deduce that there exist $X \in \mathbb{Z}$ and $Y \in \mathbb{Z}$ such that

$$aX^2 + bXY + cY^2 = \begin{cases} N & \text{if } 2 \mid \alpha, \\ 2N & \text{if } 2 \nmid \alpha. \end{cases}$$

If $2 \mid \alpha$ then

$$X^2+Y^2 \equiv a^2(X^2+Y^2) \equiv a(aX^2+bXY+cY^2) \equiv aN \equiv a(a+2) \equiv 3 \pmod 4,$$

which is impossible.

If $2 \nmid \alpha$ then $X \equiv Y \pmod 2$ and

$$\begin{aligned} X^2 + Y^2 &\equiv a^2(X^2+Y^2) \equiv a(aX^2 + (b+c)Y^2) \equiv a(2N + bY(Y-X)) \\ &\equiv 2aN \equiv 2a(a+2) \equiv 6 \pmod 8, \end{aligned}$$

which is impossible.

This completes the proof that $R_{[a,b,c]}(n,d) = 0$ for $N \equiv a+2$ (mod 4). ■

Applying Theorem 2, we obtain

COROLLARY 10. *Let* $n = 2^\alpha 41^\beta N$, *where* $(N,82) = 1$. *Then*

$$R_{[1,0,41]}(n,-164) = 0 \quad \text{if } N \equiv 3 \pmod 4.$$

COROLLARY 11. *Let* $n = 2^\alpha 41^\beta N$, *where* $(N,82) = 1$. *Then*

$$R_{[5,\pm 4,9]}(n,-164) = 0 \quad \text{if } N \equiv 3 \pmod 4.$$

COROLLARY 12. *Let* $n = 2^\alpha 7^\beta N$, *where* $(N,14) = 1$. *Then*

$$R_{[1,0,49]}(n,-196) = 0 \quad \text{if } N \equiv (-1)^{\beta-1} \pmod 4.$$

References

[1] F. van der Blij, *Binary quadratic forms of discriminant* −23, Indag. Math. 14 (1952), 498–503.
[2] D. A. Buell, *Binary Quadratic Forms*, Springer, New York, 1989.

[3] N. A. Hall, *The number of representations function for binary quadratic forms*, Amer. J. Math. 62 (1940), 589–598.
[4] J. G. Huard, P. Kaplan and K. S. Williams, *The Chowla–Selberg formula for genera*, Acta Arith. 73 (1995), 271–301.
[5] P. Kaplan and K. S. Williams, *On a formula of Dirichlet*, Far East J. Math. Sci. 5 (1997), 153–157.
[6] G. A. Lomadze, *On the representation of numbers by binary quadratic forms*, Tbiliss. Gos. Univ. Trudy Ser. Mekh.-Mat. Nauk 84 (1962), 285–290 (in Russian).
[7] —, *On the representation of numbers by positive binary diagonal quadratic forms*, Mat. Sb. (N.S.) 68 (110) (1965), 282–312 (in Russian); English transl.: Amer. Math. Soc. Transl. (2) 82 (1969), 85–122.
[8] —, *The representation of numbers by certain binary quadratic forms*, Izv. Vyssh. Uchebn. Zaved. Mat. 11 (1970), 71–75.
[9] H. Muzaffar and K. S. Williams, *A restricted Epstein zeta function and the evaluation of some definite integrals*, Acta Arith. 104 (2002), 23–66.
[10] T. V. Vephvadze [T. V. Vepkhvadze], *The representation of numbers by positive Gaussian binary quadratic forms*, Sakharth. SSR Mecn. Akad. Moambe 56 (1969), 277–280 (in Russian).
[11] —, *The representation of numbers by positive binary quadratic forms with odd discriminant*, ibid. 58 (1970), 29–32 (in Russian).
[12] —, *The representation of numbers by positive Gaussian binary quadratic forms*, Sakharth. SSR Mecn. Akad. Math. Inst. Shrom. 40 (1971), 21–58 (in Russian).
[13] —, *The representation of numbers by certain binary quadratic forms*, Thbilis. Univ. Shrom. A 1 (137) (1971), 17–24 (in Russian).
[14] —, *The representation of numbers by positive binary quadratic forms of odd discriminant*, Sakharth. SSR Mecn. Akad. Math. Inst. Shrom. 45 (1974), 5–40 (in Russian).
[15] —, *The number of representations of numbers by genera of positive binary quadratic forms*, ibid. 57 (1977), 29–39 (in Russian).
[16] —, *General theta-functions with characteristics and exact formulae for binary quadratic forms*, Bull. Georgian Acad. Sci. 154 (1996), 341–347.
[17] V. G. Zhuravlev, Review of [16], Math. Rev. 99m:11046.

Département de Mathématiques
Université de Nancy I
54506 Vandœuvre-lès-Nancy, France
E-mail: pierre.kaplan@wanadoo.fr

School of Mathematics and Statistics
Carleton University
Ottawa, Ontario, Canada K1S 5B6
E-mail: williams@math.carleton.ca

Received on 22.9.2003 (4627)