BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 43, Number 3, July 2006, Pages 285–304
S 0273-0979(06)01107-4
Article electronically published on April 14, 2006

QUADRATIC DIOPHANTINE EQUATIONS, THE CLASS NUMBER, AND THE MASS FORMULA

GORO SHIMURA

1. The basic setting and two ternary cases

We take a finite-dimensional vector space V over a field F and take also an F-bilinear symmetric form $\varphi : V \times V \to F$. We then put $\varphi[x] = \varphi(x, x)$ for $x \in V$, thus using the same letter φ for the quadratic form and the corresponding symmetric form. By a *quadratic Diophantine equation* we mean an equation of the type

$$\varphi[x] = q \tag{1}$$

with a given $q \in F^\times$. In particular, in the classical case with $F = \mathbf{Q}$ and $V = \mathbf{Q}^n$, we usually assume that φ is $\mathbf{Z}$-valued on $\mathbf{Z}^n$ and $q \in \mathbf{Z}$. The purpose of the present article is to present some new ideas on various arithmetical questions on such an equation. We start with some of our basic symbols and terminology. For a set X we denote by $\#X$ or $\#\{X\}$ the number $(\leq \infty)$ of elements of X. For an associative ring R with identity element, we denote by $R^\times$ the group of invertible elements of R and by $M_n(R)$ the ring of all square matrices of size n with entries in R. We then put $GL_n(R) = M_n(R)^\times$ and denote by 1_n the identity element of $M_n(R)$. For two square matrices A and B of size m and n we denote by $\mathrm{diag}[A, B]$ the square matrix of size $m + n$ with A and B in diagonal blocks and zeros in the remaining blocks.

Now, given (V, φ) as above, we always assume that φ is nondegenerate. We also put $n = \dim(V)$ and define, as usual, the orthogonal group $O^\varphi(V)$ and the special orthogonal group $SO^\varphi(V)$ by

$$\begin{aligned} O^\varphi(V) &= \bigl\{\alpha \in GL(V) \bigm| \varphi[x\alpha] = \varphi[x] \text{ for every } x \in V\bigr\}, \\ SO^\varphi(V) &= O^\varphi(V) \cap SL(V), \quad \text{written also } SO(\varphi) \text{ and } SO(V, \varphi). \end{aligned}$$

We let $GL(V)$ act on V on the right, so that $x\alpha$ is the image of x under α.

As the base field F we take, for the moment, an algebraic number field or its completion at a nonarchimedean prime. We denote by $\mathfrak{g}$ the ring of algebraic integers in the former case and the ring of local integers in the latter case. Those who are not much interested in the general case may assume that F is $\mathbf{Q}$ or the p-adic number field $\mathbf{Q}_p$ for any prime number p, and $\mathfrak{g}$ is $\mathbf{Z}$ or the ring $\mathbf{Z}_p$ of p-adic integers. By a $\mathfrak{g}$-*lattice* (simply a *lattice*) in V we mean a finitely generated

Received by the editors October 26, 2005.
2000 *Mathematics Subject Classification.* Primary 11E12; Secondary 11D09, 11E41.

$\mathfrak{g}$-submodule of V that spans V over F. We call a lattice L in V *integral* (with respect to φ) if $\varphi[x] \in \mathfrak{g}$ for every $x \in L$. Given a lattice L in V, we put

$$\Gamma(L) = \bigl\{\alpha \in SO^{\varphi}(V) \bigm| L\alpha = L\bigr\}. \tag{2}$$

In the simplest case we can take $V = \mathbf{Q}^n$, $L = \mathbf{Z}^n$, and $\varphi[x] = x\Phi \cdot {}^t x$ with a matrix $\Phi = (c_{ij})$ with $c_{ij} \in \mathbf{Q}$ and a row vector $x = (x_i)_{i=1}^n$. Clearly L is integral if and only if $2c_{ij} \in \mathbf{Z}$ and $c_{ii} \in \mathbf{Z}$ for every i and j; $\Gamma(L) = SO^{\varphi}(V) \cap SL_n(\mathbf{Z})$.

Let us now consider some questions about equation (1). Taking a lattice L in V, we can ask, for example, the number of elements in the set

$$L[q] = \bigl\{x \in L \bigm| \varphi[x] = q\bigr\}, \tag{3a}$$

which is an old problem investigated by many number theorists, especially when $\varphi[x] = \sum_{i=1}^n x_i^2$ and $L = \mathbf{Z}^n$. This question is preceded by a famous statement of Fermat that every natural number is the sum of at most three triangular numbers, and also of four squares, of five pentagonal numbers, etc. Though this problem is of a nature quite different from the type of problems we are going to discuss, it must be remembered that it was also a question about quadratic forms and that many mathematicians in the 18th and early 19th centuries were conscious of this problem and expended considerable effort toward its solution.

In addition to $L[q]$, there is another set which has a long history as an object of study. Namely, assuming $L = \mathbf{Z}^n$, we put

$$L^0[q] = \Bigl\{x = \{x_i\}_{i=1}^n \in L[q] \Bigm| \sum_{i=1}^n x_i\mathbf{Z} = \mathbf{Z}\Bigr\} \tag{3b}$$

and call an element of $L^0[q]$ a *primitive* solution of equation (1). In terms of matrices, the equation has the form $x\Phi \cdot {}^t x = q$, and $x = \{x_i\}_{i=1}^n$ is primitive if the x_i have no nontrivial common divisor. Notice that both $L[q]$ and $L^0[q]$ are stable under $\Gamma(L)$.

This condition of primitivity is fundamental in our theory, as will be explained later. For the moment, let us just say that the nature of the question about $L^0[q]$ is quite different from that about $L[q]$: roughly speaking, the former is more conceptual, and the latter more computational. We shall eventually explain this difference and present a new interpretation of $L^0[q]$, which leads to certain class number formulas for orthogonal groups and new mass formulas for such groups. We will also consider an equation of the type $\xi\Phi \cdot {}^t\xi = \Psi$ with another symmetric matrix Ψ of size m (instead of a scalar q) and an $(m \times n)$-matrix ξ and will develop a theory parallel to that for $\varphi[x] = q$.

We now recall an ancient problem: to find a systematic method of obtaining $x \in L[q]$ when $F = \mathbf{Q}$, $n = 2$, and $L = \mathbf{Z}^2$. Such was discussed by many mathematicians, Fermat and Euler, in particular. But all those works were restricted to some special binary forms. The case of an *arbitrary* binary form was settled by Lagrange [12] and later reformulated by Gauss [7]. In this article, however, we are *not* interested in their methods of how to find x. Indeed, what concerns us is the "conceptual meaning" of each solution of (1) when $n > 2$. Still, there are some aspects of Lagrange's work relevant to our topic. We first note that he introduced the notion of a *class* of binary forms. To be precise, take $F = \mathbf{Q}$ and $\mathfrak{g} = \mathbf{Z}$ and consider a quadratic form $\xi u^2 + \zeta uv + \eta v^2$ of two variables u, v with coefficients ξ, η, $\zeta \in \mathbf{Z}$. We then put $q = 4\xi\eta - \zeta^2$ and call $-q$ the *discriminant* of the binary form; we naturally assume that $q \neq 0$. If we represent the form by the matrix

$$h = \begin{bmatrix} \xi & \zeta/2 \\ \zeta/2 & \eta \end{bmatrix},$$

then $\det(2h) = q$. We say that another form represented by a similar matrix h' belongs to the same *class* as h if

$$h' = \det(\alpha)^{-1} \cdot \alpha h \cdot {}^t\alpha \quad \text{with } \alpha \in GL_2(\mathbf{Z}). \tag{4}$$

Here we deviate from the traditional definition $h' = \alpha h \cdot {}^t\alpha$ with $\alpha \in SL_2(\mathbf{Z})$, because (4) with $GL_2(\mathfrak{g})$ in place of $GL_2(\mathbf{Z})$ is the best definition in the case of an arbitrary number field.

Now Lagrange showed that the number of classes of the forms with a given discriminant is finite. For this and other results of Lagrange and his predecessors, the reader is referred to Weil's book [31]. For an obvious technical reason, it is natural to assume, as Lagrange and later researchers did, that the binary form is *primitive,* which means that ξ, η, ζ have no nontrivial common divisor.

In order to interprete the notion of class in a different way, we consider a *ternary* form φ defined on $\mathbf{Q}^3$ by

$$\varphi[(x, y, z)] = 4xy - z^2. \tag{5a}$$

If we fix q, then a primitive binary form of discriminat $-q$ corresponds to a primitive solution $h = (\xi, \eta, \zeta) \in \mathbf{Z}^3$ of the equation $\varphi[h] = q$ with φ of (5a), that is, an element of $L^0[q]$ with $L = \mathbf{Z}^3$. This much is trivial, but here is a nontrivial fact: $\Gamma(\mathbf{Z}^3)$ *defined by* (2) *in the present case consists of all the maps* $h \mapsto h'$ *of* (4). (It seems that the previous researchers did not connect $SO(\varphi)$ for φ of (5a) with binary forms, and the last fact on $\Gamma(\mathbf{Z}^3)$ is not a well known old result. Indeed, the corresponding fact in the case of an arbitrary number field F depends on the nature of the ideal class group of F; see [22, Lemma 12.10].) Therefore the classes of binary forms of discriminant $-q$ correspond bijectively to $L^0[q]/\Gamma(L)$ defined with respect to φ of (5a). Denoting by $c(q)$ the number of classes of primitive binary forms of discriminant $-q$, we thus obtain

$$\#\bigl\{L^0[q]/\Gamma(L)\bigr\} = c(q). \tag{5b}$$

Before discussing another ternary form, let us state here a basic result of Dedekind. Assuming that $-q$ is not a square in $\mathbf{Q}$, define a quadratic extension K of $\mathbf{Q}$ by $K = \mathbf{Q}(\sqrt{-q}\,)$. Then we can put $-q = f^2 d$ with $0 < f \in \mathbf{Z}$ and the discriminant d of K. Denote by $\mathfrak{r}$ the ring of algebraic integers in K and define a subring $\mathfrak{o}$ of $\mathfrak{r}$ by $\mathfrak{o} = \mathbf{Z} + f\mathfrak{r}$. Then Dedekind [4, §187] showed that there is a bijection from the set of all ideal classes of proper $\mathfrak{o}$-ideals onto the set of all classes of primitive binary forms of discriminat $-q$. If $-q = d$, then $f = 1$, $\mathfrak{o} = \mathfrak{r}$, and a proper $\mathfrak{o}$-ideal is a fractional ideal in K. As to later expositions of this result of Dedekind, the reader is referred to [10, §53] and [3, Chapter II, §7.5], for example. By virtue of this result, $c(q)$ is the class number of such an $\mathfrak{o}$ and, in particular, the class number of K if $-q = d$. Though the theory of proper $\mathfrak{o}$-ideals is not so complicated, we will not go into details here, as such is not essential for the understanding of our main ideas.

Next we turn to a more difficult problem concerning

$$\varphi[(x, y, z)] = x^2 + y^2 + z^2. \tag{6a}$$

We naturally look for primitive solutions h of the equation $\varphi[h] = q$ for a given $q \in \mathbf{Z}, > 0$. In this case, the permutations of (x, y, z) and the diagonal elements of $GL_3(\mathbf{Z})$ generate a group of order 48 which has $\mathit{\Gamma}(\mathbf{Z}^3)$ as a subgroup of index 2. Now Gauss showed in [7] that such a primitive solution exists if and only if $q = b^2m$ with an odd positive integer b and a squarefree positive integer m such that $m \not\equiv 7 \pmod 8$. From this he derived by a short elementary argument that every natural number is the sum of at most three triangular numbers. (It may be added that Lagrange solved the case of four squares some 30 years earlier.) These were already wonderful achievements, but he proved a far deeper result on $L^0[q]$ for such a q, which can be reformulated as follows:

$$\text{(6b)}\qquad \#\bigl\{L^0[q]/\mathit{\Gamma}(L)\bigr\} = c(q)\cdot\begin{cases}1 & \text{if } m \equiv 3 \pmod 4 \text{ or } q \le 2,\\ 2^{-1} & \text{otherwise.}\end{cases}$$

From this we can easily derive a formula valid for $q = b^2m > 3$:

$$\text{(6c)}\qquad \#L^0[q] = c(q)\cdot\begin{cases}24 & \text{if } m \equiv 3 \pmod 4,\\ 12 & \text{otherwise.}\end{cases}$$

In fact, Gauss stated something equivalent to (6c), but did not give a clear-cut statement in the form (6b). His proof is long and roundabout. In order to study a ternary equation $x\mathit{\Phi}\cdot {}^t x = q$, he considered the representation of a binary form by another ternary form, namely an equation $\xi\mathit{\Psi}\cdot {}^t\xi = \eta$, where $\mathit{\Psi}$ is such that $\mathit{\Phi} = -\det(\mathit{\Psi})\mathit{\Psi}^{-1}$ and η is a (2×2)-matrix that represents a given binary form. This technique was initiated earlier by Legendre in [13] for $\mathit{\Psi} = 1_3$, and he almost proved the results of Gauss, including the one on three triangular numbers. Though Gauss rigorously proved them, it must be remembered that he was not so original in this respect. In any case, there is a simpler method, as we will show later, and so we are tempted to say that in a sense Gauss was misled by Legendre's work. Without [13] he might have found a different, possibly shorter, proof, but of course we cannot change history, and, after all, the idea worked.

Gauss was not the only person "misled" by Legendre; indeed, Eisenstein and Minkowski employed the same method in dealing with $\#L^0[q]$ when φ is the sum of five squares. But our aim is to present new ideas which are more straightforward than their approach, and so we will not explain how they obtained their results, which are splendid in spite of the seeming awkwardness of the method. The reader is referred to Bachmann's book [1] for an exposition of this subject; see also [22, p. 137, lines 18–23] for an interpretation of their methods.

History aside, our point is that there is an unmistakable parallelism between (5b) and (6b). Therefore we can expect the existence of a general principle of which (5b) and (6b) are special cases. In the above two cases, $n = 3$ and binary forms have two variables, and so the expected principle may be of the following type:

(7) $\#\bigl\{L^0[q]/\mathit{\Gamma}(L)\bigr\}$ equals the class number of an object in dimension $n-1$.

But things are not that simple, though the idea of (7) is basically right. Also, we can seek an n-dimensional generalization of (6c), but that requires the concept of "mass". To make precise statements, we first put

$$\text{(8)}\qquad L[q,\,\mathbf{Z}] = \bigl\{x \in V \,\big|\, \varphi[x] = q,\ \varphi(x,\,L) = \mathbf{Z}\bigr\}.$$

This will replace $L^0[q]$. Notice that $L[q,\,\mathbf{Z}]$ is not defined as a subset of $L[q]$. If $\varphi[x] = x\mathit{\Phi}\cdot {}^t x$ with $\mathit{\Phi} = (c_{ij})$ and $L = \mathbf{Z}^n$, then $\varphi(x,\,L) = \sum_{i=1}^n \bigl(\sum_{j=1}^n c_{ij}x_j\bigr)\mathbf{Z}$. In particular, if $\varphi[x] = \sum_{i=1}^n x_i^2$ and $L = \mathbf{Z}^n$, then $L^0[q] = L[q,\,\mathbf{Z}]$. Next, we call

L *φ-maximal,* or simply *maximal,* if L is the only integral lattice containing itself. The lattice $\mathbf{Z}^3$ is maximal with respect to φ of (6a). As for φ of (5a), if we denote by Λ the set of all $(\xi, \eta, \zeta) \in \mathbf{Q}^3$ such that $2\xi, 2\eta, \zeta \in \mathbf{Z}$, then we easily see that Λ is maximal with respect to (5a) and $(\mathbf{Z}^3)^0[q] = \Lambda[q, \mathbf{Z}]$. Thus one of our key ideas is to consider $L[q, \mathbf{Z}]$ with a maximal L in place of $L^0[q]$.

Now the precise version of (7) is the first of the following two formulas, which form the principal results whose explanation is the main objective of this article:

$$\text{(9a)} \qquad \sum_{i\in I} \#\bigl\{L_i[q, \mathbf{Z}]/\mathit{\Gamma}(L_i)\bigr\} = \text{the class number of a group } H,$$

$$\text{(9b)} \qquad \sum_{i\in I} \#\{L_i[q, \mathbf{Z}]\}/\#\mathit{\Gamma}(L_i) \; = \; \text{the mass of } H \text{ if } \varphi \text{ is definite,}$$

provided L is maximal and $L[q, \mathbf{Z}] \neq \emptyset$. Formula (9b) is a generalization of (6c).

We have to explain what $\{L_i\}_{i\in I}$, H, the class number, and the mass are. To define H, we first pick $h \in L[q, \mathbf{Z}]$ and take the orthogonal complement W of $\mathbf{Q}h$, which we write $(\mathbf{Q}h)^\perp$ and which is defined by

$$\text{(10)} \qquad W = (\mathbf{Q}h)^\perp = \bigl\{y \in V \bigm| \varphi(h, y) = 0\bigr\}.$$

Clearly $\dim(W) = n - 1$. Now the group H in (9a, b) is given by $H = SO^\varphi(W)$, where we use φ also for its restriction to W. We view H as a subgroup of $SO^\varphi(V)$ by putting

$$\text{(11)} \qquad H = SO^\varphi(W) = \bigl\{\alpha \in SO^\varphi(V) \bigm| h\alpha = h\bigr\}.$$

In the next section we shall explain what $\{L_i\}_{i\in I}$, the class number, and the mass are. Before doing so, we should mention a natural question: Is $\#\bigl\{L^0[q]/\mathit{\Gamma}(L)\bigr\}$ or $\#\bigl\{L[q, \mathbf{Z}]/\mathit{\Gamma}(L)\bigr\}$ really finite? If φ is positive or negative definite, then $\mathit{\Gamma}(L)$, $L[q]$, and $L[q, \mathbf{Z}]$ are finite sets, as can easily be seen, and so the matter is trivial. But the finiteness of $\#\bigl\{L[q]/\mathit{\Gamma}(L)\bigr\}$ for indefinite φ is nontrivial. There is a similar question about the equation $\xi\mathit{\Phi} \cdot {}^t\xi = \mathit{\Psi}$, mentioned above, over a number field. Namely, fixing a lattice Λ in the space of $(m \times n)$-matrices, we ask whether the orbit of all such $\xi \in \Lambda$ under the stabilizer of Λ in $SO(\mathit{\Phi})$ is finite. We can even ask the same type of question over a nonarchimedean completion of F. The answer is indeed affirmative in both global and local cases; see [22, Theorems 13.2 and 13.3].

Such finiteness results, when $F = \mathbf{Q}$, were known to Siegel; also they are implicit in the convergence of the Siegel-Weil formula, though that requires the convergence condition. He always said that the fact followed from reduction theory ([27, p. 399], for example), which is true, but he never bothered himself with its proof until very late. Indeed, in [28], he treated the question of finding ξ satisfying $\xi\mathit{\Phi}\cdot{}^t\xi = \mathit{\Psi}$ over $\mathbf{Z}$ in the classical style of Lagrange; his answer includes the finiteness. It is as if he did not wish to cause later researchers to complain about this point. In any case, the facts are nontrivial, and the local case does not seem to have been previously stated.

There is another natural question: why do we consider $L^0[q]$ or $L[q, \mathbf{Z}]$ instead of $L[q]$? Before answering this question, we note here a result about $\#L[q]$ for φ of (6a) given in [21, p. 1067]. Let $q = 2^\nu r^2 t$ with $0 \leq \nu \in \mathbf{Z}$ and odd positive integers

r and t, t squarefree. Let $r = \prod_p p^{\lambda_p}$ be the prime decomposition of r. Then

$$(*) \quad \#L[q] = \begin{cases} 0 \quad \text{if } \nu \in 2\mathbf{Z} \text{ and } t - 7 \in 8\mathbf{Z}, \\ A\pi^{-1}L(1,\, \psi)rt^{1/2}\prod_p^* \left\{ \sum_{k=0}^{\lambda_p} p^{-k} - \psi(p)\sum_{i=1}^{\lambda_p} p^{-i} \right\} \text{ otherwise,} \end{cases}$$

where A is 24 or $24\sqrt{2}$ according to whether $\nu \in 2\mathbf{Z}$ or $\nu \notin 2\mathbf{Z}$, ψ is the primitive Dirichlet character corresponding to $\mathbf{Q}(\sqrt{-q}\,)$, and $\prod_p^*$ is the product over all the prime factors p of r such that $\psi(p) \neq 1$. Notice that $L(1,\, \psi)$ is the class number of $\mathbf{Q}(\sqrt{-q}\,)$ times an elementary factor (as shown by (13a) below), and so $(*)$ is similar to (6c) to some extent but far more complex. In general the formula for $\#L[q]$ for a definite φ, when n is odd, is as complicated as, and often more complicated than, $(*)$, whereas we have simpler formulas for $L^0[q]$, as can be seen from (9a). Besides, the proof of (9a) gives a conceptual explanation why the class number is involved, but we cannot do that for $L[q]$ except in some special cases. This is the main reason for our discussing $L[q,\, \mathbf{Z}]$ and $L^0[q]$.

2. The class number and mass of an orthogonal group

We are going to define the *class* and *genus* of a lattice in V. Fixing $(V,\, \varphi)$ over $\mathbf{Q}$, put $G = SO^{\varphi}(V)$. For each prime number p we put $V_p = V \otimes_{\mathbf{Q}} \mathbf{Q}_p$, extend φ to a symmetric form $\varphi_p : V_p \times V_p \to \mathbf{Q}_p$, and put $G_p = SO(V_p,\, \varphi_p)$. For a lattice L in V, we denote by L_p the $\mathbf{Z}_p$-linear span of L in V_p, which is a $\mathbf{Z}_p$-lattice in V_p.

Two lattices L and M in V are said to belong to the same *G-class* if $M = L\alpha$ with $\alpha \in G$. They belong to the same *G-genus* if $M_p = L_p\alpha_p$ with some $\alpha_p \in G_p$ for every prime number p. Now here is a basic fact:

(12) The G-genus of L consists of a finite number of G-classes of lattices.

This follows from reduction theory of Minkowski. We can define the genus and class of a $\mathfrak{g}$-lattice in the case of an arbitrary number field F in a similar way by taking nonarchimedean completions of F in place of $\mathbf{Q}_p$. Then (12) holds. We can define the G-class and G-genus for an algebraic group G over F of a more general type acting on V. Then (12) holds; see [2] for the result in the most general case.

Originally the genus and class were defined in terms of matrices; see [25], for example. They can easily be translated into those in terms of lattices defined as above, provided F has class number 1. The reader is referred to [22, §9.27] for the explanation.

Now the number of classes in the genus is called the *class number of the genus.* But this depends on the choice of L, or rather, of a genus of lattices. However, all maximal lattices form a single G-genus, and so the number of G-classes in that genus is well defined. Therefore we may call it *the class number* of $(V,\, \varphi)$, or even *the class number* of G. But the latter definition is somewhat misleading, as $SO^{\varphi}(V) = SO^{c\varphi}(V)$ for every $c \in F^{\times}$, and a φ-maximal lattice may not be $c\varphi$-maximal. A better alternative is to define the class number in terms of a certain subgroup of the adelization of G, which will be explained in Section 4.

Returning to (9a), $\{L_i\}_{i \in I}$ is a complete set of representatives for the G-classes in the G-genus of a fixed maximal lattice L, where $G = SO^{\varphi}(V)$. The right-hand side is actually the number of H-classes in the H-genus of L. Since the group H acts on the vector space W of (10), taking a maximal lattice M in W, we can consider the number of H-classes in the H-genus of M, but this may not be equal to the number of H-classes in the H-genus of L, and so (9a) is not a precise statement, though the two class numbers often coincide.

If the class number of G is 1, then the left-hand side of (9a) or (9b) consists of a single term, which is the case for the forms of (5a) and (6a), and so (5b) and (6b) are special cases of (9a). In those two cases the group H is given by $H = \{x \in K^\times \mid N_{K/\mathbf{Q}}(x) = 1\}$ with $K = \mathbf{Q}(\sqrt{-q}\,)$, and there is a simple relation between the class number of H and that of K.

The proof of (9a) is not so short, but it is conceptually straightforward; we can at least say that it is not as painful as the proof of (6c) by Gauss. But postponing the proof, let us now explain what the mass means.

The mass formula for an orthogonal group when $n = 2$ is actually Dirichlet's formulas for the class number h_K of a quadratic field K. Let us state them here in the forms given in modern textbooks, not in the original style of Dirichlet. Let $\chi(a) = \left(\frac{d}{a}\right)$ for $a \in \mathbf{Z}$, where d is the discriminant of K (and so $K = \mathbf{Q}(d^{1/2})$), and let $L(s, \chi) = \sum_{m=1}^{\infty} \chi(m)m^{-s}$ with a complex variable s. This series is convergent for $\mathrm{Re}(s) > 1$ and can be continued to an entire function. We have then

$$h_K \cdot w^{-1} = (2\pi)^{-1}|d|^{1/2} \cdot L(1, \chi) \quad \text{if} \quad d < 0, \tag{13a}$$

$$h_K \cdot \log\varepsilon = 2^{-1}|d|^{1/2} \cdot L(1, \chi) \quad \text{if} \quad d > 0. \tag{13b}$$

Here w is the number of roots of unity in K. For $d > 0$, we fix an embedding of K into $\mathbf{R}$ and take a fundamental unit $\varepsilon > 1$ in K. We can view these as special cases of the formula for the residue of the Dedekind zeta function at 1, due to Dedekind himself, which is also a kind of mass formula, but let us restrict ourselves to orthogonal groups.

The idea of the mass of a genus for $n > 2$ goes back to Eisenstein and Minkowski. We state here the mass formula essentially in Siegel's style, though we employ the definition of the mass introduced in [17] and [18]. Given a lattice L in V, we define *the mass of* $G = SO^\varphi(V)$ relative to L (or the mass of the genus of L with respect to G) to be the quantity given by

$$\mathfrak{m}(G, L) = \sum_{i\in I} \nu(\mathit{\Gamma}_i), \quad \mathit{\Gamma}_i = \mathit{\Gamma}(L_i), \tag{14a}$$

$$\nu(\mathit{\Gamma}) = \begin{cases} [\mathit{\Gamma} : 1]^{-1} & \text{if } \varphi \text{ is definite,} \\ \mathrm{vol}(\mathit{\Gamma}\backslash\mathcal{Z})/\#\big(\mathit{\Gamma} \cap \{\pm 1\}\big) & \text{otherwise.} \end{cases} \tag{14b}$$

Here L is not necessarily maximal, $\{L_i\}_{i\in I}$ is a complete set of representatives for the G-classes in the G-genus of L, and $\mathcal{Z}$ is the symmetric space on which G has a natural action; we fix a G-invariant measure on $\mathcal{Z}$. Siegel showed (for an integral $L = \mathbf{Z}^n$) in [25] and [26] that

$$\mathfrak{m}(G, L) = d_\infty \prod_p d_p, \tag{15}$$

$$d_p = \lim_{m\to\infty} p^{-mn(n-1)/2} \#\big\{\alpha \in GL_n\big(\mathbf{Z}_p/(p^m)\big) \,\big|\, \alpha\varphi \cdot {}^t\alpha \equiv \varphi \pmod{p^m}\big\}. \tag{16}$$

In fact, the right-hand side of (16) becomes constant for sufficiently large m. The number d_p is called *the representation density* at p; d_∞ is defined suitably; see [26, pp. 410–412]. But Siegel did not give a precise form of the right-hand side of (15), though he computed d_∞ and d_p for p not dividing $2\det(\varphi)$. An exact formula for

$\mathfrak{m}(G,\,L)$ when L is maximal was given in [18]. To state it, we need a few basic facts on the classification of $(V,\,\varphi)$ over $\mathbf{Q}$. We first put $\delta(\varphi) = (-1)^{n(n-1)/2}\det(\varphi)$ and call it the *discriminant* of φ. This is determined modulo the squares of the elements of $\mathbf{Q}^\times$. Next, the signature of φ as a real quadratic form is an obvious invariant. In addition, for each prime number p, once n and $\delta(\varphi)$ are given, there exist only a finite number of quadratic spaces over $\mathbf{Q}_p$, which can be explicitly described. Now $(V,\,\varphi)$ over $\mathbf{Q}$ is completely determined by the signature of φ and $(V_p,\,\varphi_p)$ for all p, a fact called *the Hasse principle.* These results can be found in almost any book on quadratic forms, [6] or [22, Section 7], for example.

To state the formula for $\mathfrak{m}(G,\,L)$, fix a maximal lattice L and denote by φ_0 the matrix that represents φ with respect to a $\mathbf{Z}$-basis of L. Then [18, Theorem 5.8] gives

$$\mathfrak{m}(G,\,L) = A\cdot\det(2\varphi_0)^\mu\prod_p\lambda_p\cdot\begin{cases}1 & \text{if } n\notin 2\mathbf{Z},\\ L(n/2,\,\psi) & \text{if } n\in 2\mathbf{Z}.\end{cases}\tag{17}$$

Here A is an elementary constant depending only on n, $\delta(\varphi)$, the signature of φ, and the choice of the measure on $\mathcal{Z}$; $\mu = (n-1)/2$, p runs over the prime factors of $\det(2\varphi_0)$, λ_p is a rational number determined by $(V_p,\,\varphi_p)$, and ψ is the primitive Dirichlet character corresponding to $\mathbf{Q}\bigl(\delta^{1/2}\bigr)$, $\delta = (-1)^{n/2}\det(\varphi_0)$. The proof of (17) relies on the fact that the mass is the residue of a certain zeta function on G, and that residue can be obtained by computing the residue of an Eisenstein series on a split orthogonal group. This may be viewed as a byproduct of the general theory of such zeta functions and is different from Siegel's proof of (15).

Suppose that the $\nu(\Gamma_i)$ are the same for all i. (This is the case if $n = 2$, as G becomes commutative.) Then we obtain

$$\#I\cdot\nu(\Gamma_1) = \text{the right-hand side of (17).}$$

If $n = 2$, this is essentially the same as (13a) or (13b), as $\#I = 2^{2-t}h_K$ if $d > 0$ and $N(\varepsilon) = 1$, and $\#I = 2^{1-t}h_K$ otherwise, where t is the number of prime factors of d and ε is a fundamental unit of K; see [22, 9.16].

In general $\nu(\Gamma_i)$ can take many different values, and so we cannot prove a clear-cut formula for $\#(I)$. We have formulas for their sum which generalize (13a, b).

If φ is indefinite, then $\mathrm{vol}(\Gamma\backslash\mathcal{Z})$ plays the role of $\log\varepsilon$. In that sense (14a) combined with (15) is of the same nature as (13a, b), though (13a, b) are simpler. In any case, for $n > 2$ there is a formula for $\mathfrak{m}(G,\,L)$ like (17), but no such formula exists for the class number. In general, it is difficult to find the class number of an orthogonal group. However, by means of formula (9a), we can determine the class number in certain cases by counting the number $\#\bigl\{L[q,\,\mathbf{Z}]/\Gamma(L)\bigr\}$. We will give examples in Theorem 3.

But before discussing this, let us note another result of Siegel concerning $\#L[q]$. To make our exposition easier, we introduce the notion of the mass of a subset X of V, written $\mathfrak{m}(X)$. We take a set X of the form $X = \bigsqcup_{j=1}^k h\beta_j\Gamma$ with $\Gamma = \Gamma(L)$ and a finite subset $\{\beta_j\}$ of G. Then we put

$$\mathfrak{m}(X) = \sum_{j=1}^k \nu(\Delta_j)/\nu(\Gamma),\quad \Delta_j = \beta_j\Gamma\beta_j^{-1}\cap H.\tag{18}$$

It can easily be seen that $\mathfrak{m}(X) = \#X$ if φ is definite. Now, for $L = \mathbf{Z}^n$ Siegel showed in [25] and [26] that

$$\begin{aligned} &\mathfrak{m}(G,\, L)^{-1} \sum_{i\in I} \nu(\varGamma_i)\mathfrak{m}\bigl(L_i[q]\bigr) = e_\infty \prod_p e_p, \ \ \varGamma_i = \varGamma(L_i), \\ &e_p = \lim_{m\to\infty} p^{m(1-n)} \#\bigl\{x \in \bigl(\mathbf{Z}/p^m\mathbf{Z}\bigr)^n \bigm| \varphi[x] - q \in p^m\mathbf{Z}\bigr\}. \end{aligned} \tag{19}$$

The right-hand side becomes constant for sufficiently large m. The number e_p is called *the representation density of* q *by* φ *at* p; e_∞ is a similar density at ∞ defined by means of certain volumes. Thus, if φ is definite, then

$$\Bigl\{\sum_{i\in I} [\varGamma_i : 1]^{-1}\Bigr\}^{-1} \sum_{i\in I} [\varGamma_i : 1]^{-1} \#L_i[q] = e_\infty \prod_p e_p. \tag{20}$$

In particular, if $\#I = 1$, then $\#L[q] = e_\infty \prod_p e_p$. If $\#I > 1$, however, only the weighted average of $\bigl\{\#L_i[q]\bigr\}_{i\in I}$ can be given.

How can one compute $e_\infty \prod_p e_p$? Siegel did a few easy cases. An explicit formula was given in [19] when F is totally real, φ is totally definite, and L is maximal:

$$e_\infty \prod_p e_p = Bq^{(n-2)/2} \prod_p{}'' \varepsilon_p \cdot \begin{cases} L(n/2,\, \psi)^{-1} & (n \in 2\mathbf{Z}), \\ L\bigl((n-1)/2, \psi_q\bigr) & (n \notin 2\mathbf{Z}). \end{cases} \tag{21}$$

Here B is an elementary factor depending only on φ and independent of q; ε_p is a rational expression in $p^{n/2}$; $\prod_p''$ is the product over all prime factors p of $q \cdot \det(2\varphi_0)$, where φ_0 is as in (17); ψ is the same as in (17); ψ_q is the primitive Dirichlet character corresponding to $\mathbf{Q}(\kappa^{1/2})$, where $\kappa = q\delta(\varphi)$. The lattice L must be maximal. We prove (21) by using the fact that $e_\infty \prod_p e_p$ is a Fourier coefficient of a certain Eisenstein series. Thus the weighted average is computable by means of (21), but there is no formula for each individual $\#L_i[q]$ in general (unless $\#I = 1$). In fact, however, the quantity of (21) is a good approximation to $\#L_i[q]$. These points will be explained in Section 6. Also, it should be mentioned that (21) does not apply to the case of the sum of n squares with $L = \mathbf{Z}^n$ if $n > 3$, as $\mathbf{Z}^n$ is not maximal in such cases. Even so, the problem can be handled, as will be explained in Section 6, (R1).

3. Precise forms of the main formulas

Let us now present precise forms of (9a, b). We take $(V,\, \varphi)$ over an arbitrary number field F. (Of course the reader may assume that $F = \mathbf{Q}$.) For a $\mathfrak{g}$-lattice Λ in V, an element q in $F^\times$, and a fractional ideal $\mathfrak{b}$ in F, we put

$$\Lambda[q,\, \mathfrak{b}] = \bigl\{\, x \in V \,|\, \varphi[x] = q, \quad \varphi(x,\, \Lambda) = \mathfrak{b} \,\bigr\}. \tag{22}$$

If $F = \mathbf{Q}$, we take $\mathfrak{b} = r\mathbf{Z}$ with $r \in \mathbf{Q}^\times$; thus (22) includes (8) as a special case. It should be noted that $\Lambda[q,\, \mathfrak{b}]$ is not necessarily contained in Λ, even when $\mathfrak{b} \subset \mathfrak{g}$.

We fix a maximal lattice L, take $h \in V$ such that $q = \varphi[h] \neq 0$, and put $\mathfrak{b} = \varphi(h,\, L)$. (This means: take q and $\mathfrak{b}$ so that $L[q,\, \mathfrak{b}] \neq \emptyset$, and take $h \in L[q,\, \mathfrak{b}]$.) Put $W = (Fh)^\perp$, that is,

$$W = \bigl\{x \in V \bigm| \varphi(h,\, x) = 0\bigr\}. \tag{23}$$

Then put $G = SO^{\varphi}(V)$ and $H = SO^{\varphi}(W)$, where we use the letter φ also for its restriction to W. We view H as a subgroup of G as in (11). From Witt's theorem on quadratic forms we easily obtain

$$\#\bigl\{\{x \in V \bigm| \varphi[x] = q\}/G\bigr\} \le 1 \ \text{if}\, q \ne 0 \,\text{and}\, n > 1. \tag{24}$$

Since H acts on V, we can define the H-class and the H-genus of a lattice in V. Now (9a, b) can be given in stronger and more precise forms as follows.

Theorem 1. *Let L, h, $\mathfrak{b}$, W, and H be as above. Let $\{L_i\}_{i\in I}$ be a complete set of representatives for the G-classes in the G-genus of L. Then there exists a bijection from $\bigsqcup_{i\in I}\bigl\{L_i[q,\,\mathfrak{b}]/\Gamma(L_i)\bigr\}$ onto the set of H-classes in the H-genus of L, and therefore*

$$\sum_{i\in I}\#\{L_i[q,\,\mathfrak{b}]/\Gamma(L_i)\} = \textit{the number of } H\textit{-classes in the } H\textit{-genus of } L. \tag{25}$$

$$\sum_{i\in I}\#L_i[q,\,\mathfrak{b}]/\#\Gamma(L_i) = \textit{the mass of } H \textit{ relative to } L \textit{ if } \varphi \textit{ is totally definite.} \tag{26}$$

Here the total definiteness means that F is totally real and φ is positive or negative definite at all archimedean primes of F. The mass of H relative to L is $\sum_{j\in J}[\Delta(M_j) : 1]^{-1}$, where $\{M_j\}_{j\in J}$ is a complete set of representatives for the H-classes in the H-genus of L and $\Delta(M_j) = \bigl\{\alpha \in H \bigm| M_j\alpha = M_j\bigr\}$. This is similar to (14a).

If $\{L_i\}_{i\in I}$ consists only of L (which is the case in the setting of (5a, b) or (6a, b)), the left-hand side of (25) is $\#\bigl\{L[q,\,\mathfrak{b}]/\Gamma(L)\bigr\}$, and equality (25) in this case is a precise version of (7). In general, $L_i[q,\,\mathfrak{b}]$ may be empty for some $i \in I$.

The bijection in the theorem can be given as follows. Given $k \in L_i[q,\,\mathfrak{b}]$, we can find, by (24), an element α of G such that $k = h\alpha$. Then we can show that $L_i\alpha^{-1}$ belongs to the H-genus of L, and so we assign the H-class of $L_i\alpha^{-1}$ to k. This gives the desired bijection.

The crucial point in the proof of Theorem 1 is the following local result.

Theorem 2. *Let L be a maximal lattice in V and p a prime number. If $h,\,k \in V_p$, $\varphi[h] = \varphi[k]$, and $\varphi(h,\,L_p) = \varphi(k,\,L_p)$, then there exists an element γ of $SO(V_p,\,\varphi_p)$ such that $h\gamma = k$ and $L_p\gamma = L_p$.*

In other words, the local analogue of $L[q,\,\mathfrak{b}]$, if nonempty, consists of a single orbit under the local analogue of $\Gamma(L)$. The fact can be generalized to the case of a number field. This theorem is stated in [22, Theorem 10.5] under the condition that $\det(\varphi_p)$ is a square times a unit if n is odd, but actually that condition is unnecessary, as will be shown in [24]. In any case, the proof of Theorem 2 is long. We first classify the structures $(V,\,\varphi,\,L)$ over a local field F as follows. Denoting by $\mathfrak{g}$ the valuation ring of F, we can put

$$V = \sum_{i=1}^{r}(Fe_i + Ff_i) \oplus Z, \qquad L = \sum_{i=1}^{r}(\mathfrak{g}e_i + \mathfrak{g}f_i) \oplus M,$$
$$2\varphi(e_i,\,f_j) = \delta_{ij}, \quad \varphi(e_i,\,e_j) = \varphi(f_i,\,f_j) = 0, \quad 0 \le n - 2r = t = \dim(Z) \le 4.$$
$$\varphi[z] \ne 0 \text{ if } 0 \ne z \in Z, \quad M \text{ is a maximal lattice in } Z.$$

The structure $(V,\,\varphi,\,L)$ is determined by $(r,\,Z)$. If we denote by ζ the restriction of φ to Z, then $(Z,\,\zeta)$ is determined by $\delta(\zeta)$ if $t \ne 2$; for $t = 2$, there are exactly two types of $(Z,\,\zeta)$ with the same $\delta(\zeta)$. (For these, see [6] and [22, §§6 and 7].) Then we prove Theorem 2 (in a generalized form) for each type of $(V,\,\varphi,\,L)$; we have to treat the cases separately according to the nature of the ideal $q\mathfrak{g}$ and also to whether or not the prime ideal $\mathfrak{p}$ divides 2. For instance, take the simplest case in which $\varphi[h] = q \in \mathbf{Z}_p^\times$, $p \neq 2$, and $\varphi(h,\,L_p) = \mathbf{Z}_p$. Then we have $L_p = \mathbf{Z}_p h \oplus \bigl(L_p \cap (\mathbf{Q}_p h)^\perp\bigr)$, from which we easily obtain the desired fact.

Once Theorem 2 is established, Theorem 1 can be proved easily; see the proof of [22, Theorems 11.6 and 13.12]. Also, Theorem 2 is analogous to the fact that every local ideal is a principal ideal; that is, the local class number is always 1. It may be emphasized that the proof of Theorem 1 is purely arithmetic and involves no analysis. Formulas (5b) and (6b) are special cases of (25), and (6c) is a special case of (26). In such cases, $H = \bigl\{x \in K \bigm| N_{K/\mathbf{Q}}(x) = 1\bigr\}$ with a quadratic field K.

If $F = \mathbf{Q}$ and $\mathfrak{g} = \mathbf{Z}$, it is natural to consider $L[q,\,\mathbf{Z}]$, but the matter is not so simple. First of all, it is a highly nontrivial question to determine for which value of q the set $L[q,\,\mathbf{Z}]$ is not empty, as can be seen from the case of the sum of three squares. Indeed, it is nontrivial, if elementary, to settle this point and to show that the right-hand side of (25) in this case can be given as in (6b); the reader is referred to [22, pp. 118–119]. Next, it is not always best to formulate the result with respect to a $\mathbf{Z}$-basis of L. We will illustrate these points by numerical examples in Theorem 6.

Let us now state several consequences of Theorem 1 in the following four theorems.

Theorem 3. (i) *Suppose $n \geq 7$ and the class number of F in the narrow sense is odd. Suppose also that φ represents 0 nontrivially at an archimedean prime of F, and the same holds for the restriction of φ to W. Then $\#\bigl\{L[q,\,\mathfrak{b}]/\Gamma(L)\bigr\} = 1$.*

(ii) *Suppose $F = \mathbf{Q}$ and $\varphi[x] = \sum_{i=1}^n x_i^2$ with $n = 5,\,7,$ or 9. Let L be a maximal $\mathbf{Z}$-lattice in $V = \mathbf{Q}^n$ and q an odd prime number. If $n > 5$, suppose $q = |d_K|$, where d_K is the discriminant of $K = \mathbf{Q}(\sqrt{\kappa}\,)$, $\kappa = (-1)^{(n-1)/2}q$. Then $L[q,\,\mathbf{Z}] \neq \emptyset$, and $\#\bigl\{L[q,\,\mathbf{Z}]/\Gamma(L)\bigr\}$ equals the class number of $SO(\psi)$ with respect to the stabilizer of a maximal lattice in $\mathbf{Q}^{n-1}$, where $\psi = \mathrm{diag}[1_{n-4},\,q1_3]$.*

For the proof, see [22, Lemma 12.13, Theorems 12.1 and 12.14]. We note here only that (i) follows from (25) combined with strong approximation.

It seems that the result of Dedekind mentioned in the paragraph after (5b) has not been generalized in a clear-cut form over an arbitrary algebraic number field F. Therefore let us now consider binary forms $ax^2 + bxy + cy^2$ over F and present a generalization of (5b). We consider $(V,\,\varphi)$ by taking $V = \bigl\{h \in M_2(F) \bigm| {}^t h = h\bigr\}$ and by putting $\varphi[h] = \det(h)$ for $h \in V$. We associate the element

$$h = \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}$$

of V to the form $ax^2+bxy+cy^2$; then $-\varphi[2h] = b^2 - 4ac$, which is the discriminant of the binary form. For $\Lambda = M_2(\mathfrak{g}) \cap V$, an element $q \in F^\times$, and a fractional ideal $\mathfrak{b}$ we consider the elements $h \in V$ such that $\varphi[h] = q$ and $\varphi(h,\,\Lambda) = \mathfrak{b}$, which constitute the set $\Lambda[q,\,\mathfrak{b}]$. Let $\varDelta$ be the group of all transformations $x \mapsto \det(\alpha)^{-1} \cdot {}^t\alpha x \alpha$ with $\alpha \in GL_2(\mathfrak{g})$. Then we can prove:

Theorem 4. *Suppose $\Lambda[q,\,\mathfrak{b}] \neq \emptyset$ and $-q$ is not a square in F. Then there exists an order $\mathfrak{f}$ of discriminant $q\mathfrak{b}^{-2}$ in the field $F(\sqrt{-q}\,)$. Moreover, $\#\bigl\{\Lambda[q,\,\mathfrak{b}]/\varDelta\bigr\} =$*

$\varepsilon c(\mathfrak{f})/c_F$, where $c(\mathfrak{f})$ is the class number of $\mathfrak{f}$, c_F is the class number of F, $\varepsilon = 2$ if all archimedean and nonarchimedean primes of F are unramified in $F(\sqrt{-q}\,)$, and $\varepsilon = 1$ otherwise.

Though this is essentially a special case of (25), we need to reformulate it in terms of the even Clifford group of (V, φ); see [22, Theorem 12.9]. If $F = \mathbf{Q}$ and $\mathfrak{b} = \mathbf{Z}$, Theorem 4 gives the result of Dedekind and also (5b). It can be shown that $[\varGamma(\Lambda) : \varDelta]$ equals the number of the ideal classes in F whose squares are the principal class; see [22, Lemma 12.10]. Also, if $q\mathfrak{b}^{-2}$ is the discriminant of an order in $F(\sqrt{-q}\,)$ and c_F is odd, then $\Lambda[q, \mathfrak{b}] \neq \emptyset$, but in general $\Lambda[q, \mathfrak{b}]$ can be empty even when such an order exists.

Theorem 5. *Let n, φ, and L be as in Theorem* 3 (ii)*; let $K = \mathbf{Q}(\sqrt{\kappa}\,)$, $\kappa = (-1)^{(n-1)/2}q$, with a squarefree positive integer q; let $L(s, \chi)$ be the L-function of the primitive Dirichlet character χ corresponding to K. Then*

$$\#L[q, 2^{-1}\mathbf{Z}] = A_n(q)q^{(n-2)/2}(2\pi)^{-m}L(m, \chi),$$
$$\#L[q, \mathbf{Z}] = c_n(q) \cdot \#L[q, 2^{-1}\mathbf{Z}].$$

Here $m = (n-1)/2$, $0 < A_n(q) \in \mathbf{Z}$, and $0 \le c_n(q) \in \mathbf{Q}$; the numbers $A_n(q)$ and $c_n(q)$ are determined explicitly by q (mod 8) *and n. For example,*

$$A_7(q) = 2^9 \cdot 3^2 \cdot 7 \quad \textit{and} \quad c_7(q) = 0 \quad \textit{if} \quad q - 3 \notin 4\mathbf{Z},$$
$$A_9(q) = 2^9 \cdot 3^2 \cdot 5 \cdot 17 \quad \textit{and} \quad c_9(q) = 1/136 \quad \textit{if} \quad q - 5 \in 8\mathbf{Z}.$$

This theorem will be explained in Section 6, (R2).

As we said earlier, it is not always best to formulate the result with respect to a $\mathbf{Z}$-basis of L. To see this, first take the standard basis $\{e_i\}_{i=1}^n$ of $\mathbf{Z}^n = L$ and define a matrix $\varPhi$ by $\varPhi = [\varphi(e_i, e_j)]_{i,j=1}^n$; put $f_i = e_i\varPhi^{-1}$ and

$$\widetilde{L} = \{\, x \in V \mid 2\varphi(x, L) \subset \mathbf{Z} \,\}.$$

Then $2\widetilde{L} = \sum_{i=1}^n \mathbf{Z}f_i$ and $\varGamma(\widetilde{L}) = \varGamma(L)$. Let $h \in L[q, \mathbf{Z}]$ with $q \in \mathbf{Q}^\times$. Then $h \in 2\widetilde{L}$, and so $h = \sum_{i=1}^n a_i f_i$ with $a_i \in \mathbf{Z}$. We easily see that $h \in L[q, \mathbf{Z}]$ if and only if $\sum_{i=1}^n a_i\mathbf{Z} = \mathbf{Z}$, and also that $\varPhi^{-1} = [\varphi(f_i, f_j)]_{i,j=1}^n$. This means that

$$L[q, \mathbf{Z}] = \left\{ h = \sum_{i=1}^n a_i f_i \;\Big|\; a\varPhi^{-1} \cdot {}^t a = q,\ \sum_{i=1}^n a_i\mathbf{Z} = \mathbf{Z} \right\}, \quad a = (a_i)_{i=1}^n.$$

Therefore if we follow the traditional definition of primitivity, we have to use the matrix $\varPhi^{-1}$ instead of $\varPhi$. Take, for example, $n = 3$ and

$$2\varPhi = \mathrm{diag}\left[2,\ \begin{bmatrix} 4 & -1 \\ -1 & 2 \end{bmatrix}\right], \qquad 7\varPhi^{-1} = \mathrm{diag}\left[7,\ \begin{bmatrix} 4 & 2 \\ 2 & 8 \end{bmatrix}\right].$$

Then the result about $L[q, \mathbf{Z}]$ can be stated in terms of the equation $a\varPhi^{-1} \cdot {}^t a = q = s/7$ with $s \in \mathbf{Z}$ and $a \in \mathbf{Z}^3$ as follows.

Theorem 6. *For $0 < s \in \mathbf{Z}$ put $K = \mathbf{Q}(\sqrt{-s}\,)$. Then a vector (a, b, c) such that*

$$7a^2 + 4(b^2 + bc + 2c^2) = s \quad \textit{and} \quad a\mathbf{Z} + b\mathbf{Z} + c\mathbf{Z} = \mathbf{Z}$$

exists if and only if $s = r^2 m$ with a positive integer r and a squarefree positive integer m such that 7 does not split in K, $7 \nmid r$, and $2|r$ if $m + 1 \notin 4\mathbf{Z}$. Moreover, *the number of such* $(a,\, b,\, c)$ *equals*

$$\frac{2^{3-\mu}h_K}{w}\cdot f\prod_{p|f}\left\{1-\left(\frac{-m}{p}\right)p^{-1}\right\}.$$

Here w *is the number of roots of unity in* K*,* $\mu = 1$ *if* $7|m$ *and* $\mu = 0$ *otherwise,* h_K *is the class number of* K*,* $f = r$ *if* $m+1 \in 4\mathbf{Z}$ *and* $f = r/2$ *otherwise.*

In fact, this concerns one of the 30 ternary forms for which we can determine exactly when $L[q,\, \mathbf{Z}] \neq \emptyset$ and also $\#L[q,\, \mathbf{Z}]$. The details will be given in [24].

4. Formulation in terms of adeles and generalizations

Let us now formulate various things in terms of the adelization $G_{\mathbf{A}}$ of G, assuming that the reader is familiar with that notion. An easy introduction to this topic can be found in [17, Section 8]. We denote by $\mathbf{a}$ and $\mathbf{h}$ the sets of archimedean primes and nonarchimedean primes of F respectively, and put $\mathbf{v} = \mathbf{a}\cup\mathbf{h}$. Given an algebraic group G defined over F, we define G_v for each $v \in \mathbf{v}$ and the adelization $G_{\mathbf{A}}$ as usual and view G and G_v as subgroups of $G_{\mathbf{A}}$. (We do not use the symbol $G_{\mathbf{Q}}$ or G_F.) We then denote by $G_{\mathbf{a}}$ and $G_{\mathbf{h}}$ the archimedean and nonarchimedean factors of $G_{\mathbf{A}}$, respectively. For $x \in G_{\mathbf{A}}$ we denote by x_v its projection to G_v.

Take $G = SO(\varphi)$, though we can take G to be an arbitrary reductive algebraic subgroup of $GL(V)$. For $x \in G_{\mathbf{A}}$ and a lattice L in V we denote by Lx the lattice in V such that $(Lx)_v = L_v x_v$ for every $v \in \mathbf{h}$. Define a subgroup U of $G_{\mathbf{A}}$ by $U = \{x \in G_{\mathbf{A}} \,|\, Lx = L\}$. This means $U = G_{\mathbf{a}}\prod_{v\in\mathbf{h}} U_v$, $U_v = \{x \in G_v \,|\, L_v x = L_v\}$. Clearly $xU \mapsto Lx^{-1}$ gives a surjection of $G_{\mathbf{A}}/U$ onto the genus of L. Therefore the map gives a bijection of $G\backslash G_{\mathbf{A}}/U$ onto the set of classes in that genus. Thus $\#(G\backslash G_{\mathbf{A}}/U)$ is the class number of the genus of L.

More generally, given an open subgroup D of $G_{\mathbf{A}}$ containing $G_{\mathbf{a}}$ and such that $D \cap G_{\mathbf{h}}$ is compact, we put $\Gamma^a = G \cap aDa^{-1}$ for every $a \in G_{\mathbf{A}}$. Let $C_{\mathbf{a}}$ be a maximal compact subgroup of $G_{\mathbf{a}}$ and let $\mathcal{Z} = G_{\mathbf{a}}/C_{\mathbf{a}}$. Then $\mathcal{Z}$ is a symmetric space on which G acts through its projection into $G_{\mathbf{a}}$. Taking a complete set of representatives $\mathcal{B}$ for $G\backslash G_{\mathbf{A}}/D$, we put

$$\mathfrak{m}(G,\, D) = \mathfrak{m}(D) = \sum_{a\in\mathcal{B}} \nu(\Gamma^a). \tag{27}$$

Here $\nu(\Gamma)$ is a quantity defined by

$$\nu(\Gamma) = \begin{cases} [\Gamma : 1]^{-1} & \text{if } G_{\mathbf{a}} \text{ is compact,} \\ \mathrm{vol}(\Gamma\backslash\mathcal{Z})/\#(\Gamma\cap T) & \text{otherwise,} \end{cases} \tag{27a}$$

where $T = \{\alpha \in G \,|\, \alpha = \text{id. on } \mathcal{Z}\}$, and we fix a Haar measure on $G_{\mathbf{a}}$, which determines a unique $G_{\mathbf{a}}$-invariant measure on $\mathcal{Z}$ by a well known principle; see (37) below. (We can give a uniform definition of $\nu(\Gamma)$ by understanding that $\mathrm{vol}(\Gamma\backslash\mathcal{Z}) = [\Gamma : \Gamma\cap T]^{-1}$ if $G_{\mathbf{a}}$ is compact.) We easily see that $\mathfrak{m}(D)$ does not depend on the choice of $\mathcal{B}$. We call $\mathfrak{m}(G,\, D)$ *the mass of* G *relative to* D. This coincides with the mass defined by (14a) if $D = \{x \in G_{\mathbf{A}} \,|\, Lx = L\}$. Also, $\#\mathcal{B}$ may be called the class number of G with respect to D. In Theorem 9 we shall give more conceptual definitions of $\mathfrak{m}(D)$ and $\nu(\Gamma)$. If $G_{\mathbf{a}}$ is compact, we have

$$\mathfrak{m}(G,\, D) = \mathfrak{m}(D) = \sum_{a\in\mathcal{B}} [\Gamma^a : 1]^{-1}. \tag{28}$$

Let us now present generalizations of (25) and (26) to the case of a Diophantine equation of the form $\xi\varPhi\cdot{}^t\xi = \varPsi$ with a nonscalar $\varPsi$ mentioned in Section 1. Instead of a matrix $\varPsi$, take a quadratic space $(X,\, \psi)$ over F of dimension $m\ \ (< n)$, and put $\mathcal{V} = \mathrm{Hom}(X,\, V)$. For $u \in \mathcal{V}$ we define $\varphi[u]$ to be a quadratic form on X defined by $\varphi[u][x] = \varphi[xu]$ for every $x \in X$. (In other words, $\varphi[u] = u\varphi\cdot{}^t u$.) We look for u such that $\varphi[u] = \psi$. Fixing $h \in \mathcal{V}$ such that $\varphi[h] = \psi$, put $W = (Xh)^{\perp}$, $G = SO^{\varphi}(V)$, and $H = SO^{\varphi}(W)$. Clearly $\dim(W) = n - m$. We have

$$\big\{k \in \mathcal{V} \,\big|\, \varphi[k] = \varphi[h]\big\} = h\cdot G. \tag{29}$$

This is a generalization of (24) and follows easily from the Witt theorem. We identify H with $\big\{\alpha \in G \,\big|\, h\alpha = h\big\}$. For $x \in G_{\mathbf{A}}$ and $h \in \mathcal{V}$ the symbol hx is meaningful as an element of $\mathcal{V}_{\mathbf{A}}$, and so $h\varXi$ is meaningful as a subset of $\mathcal{V}_{\mathbf{A}}$ for any subset $\varXi$ of $G_{\mathbf{A}}$. Then $\mathcal{V} \cap h\varXi$ is meaningful.

Theorem 7. *The symbols h, W, G and H being as above, let $D = D_0 G_{\mathbf{a}}$ with an open compact subgroup D_0 of $G_{\mathbf{h}}$. Then the following assertions hold.*

(i) *For $y \in G_{\mathbf{A}}$ we have $H_{\mathbf{A}} \cap GyD \neq \emptyset$ if and only if $\mathcal{V} \cap hDy^{-1} \neq \emptyset$.*

(ii) *Fixing $y \in G_{\mathbf{A}}$, for every $\varepsilon \in H_{\mathbf{A}} \cap GyD$ take $\alpha \in G$ so that $\varepsilon \in \alpha yD$. Then the map $\varepsilon \mapsto h\alpha$ gives a bijection of $H\backslash(H_{\mathbf{A}} \cap GyD)/(H_{\mathbf{A}} \cap D)$ onto $(\mathcal{V} \cap hDy^{-1})/\varGamma^y$, where $\varGamma^y = G \cap yDy^{-1}$.*

(iii) *Take $Y \subset G_{\mathbf{A}}$ so that $G_{\mathbf{A}} = \bigsqcup_{y\in Y} GyD$. Then*

$$\#\big\{H\backslash H_{\mathbf{A}}/(H_{\mathbf{A}} \cap D)\big\} = \sum_{y\in Y} \#\big\{(\mathcal{V} \cap hDy^{-1})/\varGamma^y\big\}. \tag{30}$$

Proof. It is not very difficult to prove (i) and (ii); the only essential point is (29). The details of the proof will be given in [24]. Once (ii) is established, (iii) follows from the fact that $H_{\mathbf{A}} = \bigsqcup_{y\in Y}(H_{\mathbf{A}} \cap GyD)$. □

We are tempted to call the set $\mathcal{V} \cap hD$ *the genus* of h. Then $\#\big\{(\mathcal{V} \cap hD)/\varGamma\big\}$ may be called the *number of classes* in that genus.

Now (30) is a generalization of (25). Before explaining that point, let us present a generalization of (26). This requires a generalization of $\mathfrak{m}(X)$ of (18). We consider a subset S of $\mathcal{V}$ of the form $S = \bigsqcup_{\zeta\in Z} h\zeta\varGamma$, where h is as above, Z is a finite subset of G, and $\varGamma = G \cap D$ with D as in the above theorem. Then we put

$$\mathfrak{m}(S) = \sum_{\zeta\in Z} \nu(\varDelta_\zeta)/\nu(\varGamma), \quad \varDelta_\zeta = H \cap \zeta\varGamma\zeta^{-1} \tag{31}$$

and call $\mathfrak{m}(S)$ the *mass* of S. Here, to define $\nu(\varDelta_\zeta)$, we need to fix a measure on $H_{\mathbf{a}}$. Thus $\mathfrak{m}(S)$ depends on the choice of measures on $G_{\mathbf{a}}$ and $H_{\mathbf{a}}$, but $\mathfrak{m}(S)$ is independent of the choice of Z and $\varGamma$, as will be shown in Section 5. (Let $\mathfrak{Y} = \big\{x \in \mathcal{V}_{\mathbf{a}} \,\big|\, \varphi[x] = q\big\}$. Since $\mathfrak{Y}$ can be identified with $H_{\mathbf{a}}\backslash G_{\mathbf{a}}$, once a measure on $G_{\mathbf{a}}$ is fixed, a measure on $\mathfrak{Y}$ determines a measure on $H_{\mathbf{a}}$, and vice versa. The replacement of h by an element of hG changes the group H, but that does not change $\mathfrak{m}(S)$ if we start with a fixed measure on $\mathfrak{Y}$. Notice also that an identification of $\mathcal{V}_{\mathbf{a}}$ with a Euclidean space determines a $G_{\mathbf{a}}$-invariant measure on $\mathfrak{Y}$.) Since the left-hand side of (30) is finite, we see that $(\mathcal{V} \cap hDy^{-1})/\varGamma^y$ is a finite set for every $y \in G_{\mathbf{A}}$. Thus we can define $\mathfrak{m}(\mathcal{V} \cap hDy^{-1})$ for every $y \in G_{\mathbf{A}}$.

If $G_{\mathbf{a}}$ is compact, we naturally take the measures of $G_{\mathbf{a}}$ and $H_{\mathbf{a}}$ to be 1. Then $\mathfrak{m}(S)$ can be defined in a unique way. We easily see that $S = \bigsqcup_{\zeta\in Z}\bigsqcup_{\gamma\in\varDelta'_\zeta\backslash\varGamma} h\zeta\gamma$, where $\Delta'_\zeta = \zeta^{-1}\Delta_\zeta\zeta$, and so $\#S = \sum_{\zeta\in Z}[\Gamma : \Delta'_\zeta] = \mathfrak{m}(S)$ if $G_{\mathbf{a}}$ is compact. Thus we obtain

$$\mathfrak{m}(S) = \#(S) \ \text{ if } \ G_{\mathbf{a}} \text{ is compact.} \tag{32}$$

Theorem 8. *The notation being the same as in Theorem 7, we have*

$$\mathfrak{m}(H,\, H_{\mathbf{A}} \cap D) = \sum_{y\in Y} \nu(\Gamma^y)\mathfrak{m}(\mathcal{V} \cap hDy^{-1}). \tag{33}$$

Proof. Let $E_y = H\backslash(H_{\mathbf{A}} \cap GyD)/(H_{\mathbf{A}} \cap D)$. For each $\varepsilon \in E_y$ take $\zeta_\varepsilon \in G$ so that $\varepsilon \in \zeta_\varepsilon yD$. By (ii) of Theorem 7 we obtain $\mathcal{V} \cap hDy^{-1} = \bigsqcup_{\varepsilon\in E_y} h\zeta_\varepsilon\Gamma^y$. Then we obtain (33) by several lines of easy calculations; see [24] for details. □

To explain that (30) and (33) are generalizations of (25) and (26), take $m = 1$, $X = F$, and $\psi[u] = qu^2$ for $u \in F$ with a fixed $q \in F^\times$. Then every element k of V defines an element of $\mathcal{V} = \mathrm{Hom}(F,\, V)$ that maps u to uk. Thus we can put $\mathcal{V} = V$. Fix $h \in V$ such that $\varphi[h] = q \in F^\times$, put $G = SO^\varphi(V)$, $W = (Fh)^\perp$, and $H = \{\alpha \in G \,|\, h\alpha = h\} = SO^\varphi(W)$. Take $\{y_i\}_{i\in I} \subset G_{\mathbf{A}}$ so that $G_{\mathbf{A}} = \bigsqcup_{i\in I} Gy_iD$, and put $\Gamma_i = G \cap y_iDy_i^{-1}$. Then (30) and (33) can be written

$$\#\{H\backslash H_{\mathbf{A}}/(H_{\mathbf{A}} \cap D)\} = \sum_{i\in I} \#\{[V \cap hDy_i^{-1}]/\Gamma_i\}, \tag{34a}$$

$$\mathfrak{m}(H,\, H_{\mathbf{A}} \cap D) = \sum_{i\in I} \#\{V \cap hDy_i^{-1}\}/\#\Gamma_i \quad \text{if } G_{\mathbf{a}} \text{ is compact.} \tag{34b}$$

Here D is arbitrary, but now we fix a maximal lattice L in V and take $D = \{x \in G_{\mathbf{A}} \,|\, Lx = L\}$. Then Theorem 2 implies that if $h \in L[q,\, \mathfrak{b}]$, then $L[q,\, \mathfrak{b}] = V \cap hD$. More generally we can prove (see [24] for the proof)

$$V \cap hDy^{-1} = (Ly^{-1})[q,\, \mathfrak{b}] \ \text{ for every } y \in G_{\mathbf{A}} \ \text{ if } n > 2 \text{ and } h \in L[q,\, \mathfrak{b}]. \tag{35}$$

Combining this result with (34a, b) and putting $L_i = Ly_i^{-1}$, we obtain

$$\#\{H\backslash H_{\mathbf{A}}/(H_{\mathbf{A}} \cap D)\} = \sum_{i\in I} \#\{L_i[q,\, \mathfrak{b}]/\Gamma_i\}, \tag{36a}$$

$$\mathfrak{m}(H,\, H_{\mathbf{A}} \cap D) = \sum_{i\in I} \#\{L_i[q,\, \mathfrak{b}]\}/\#\Gamma_i \quad \text{if } G_{\mathbf{a}} \text{ is compact.} \tag{36b}$$

These are exactly (25) and (26). Now the sum of the left-hand side of (20) is similar to the sum of (36b): we have $L_i[q,\, \mathfrak{b}]$ in (36b) instead of $L_i[q]$ in (20). But there is another essential difference between (20) and (36b): namely the right-hand side of (20) is the infinite product of type (19), but the right-hand side of (36b) is the mass of an $(n-1)$-dimensional group H. It can happen that $H_{\mathbf{A}} \cap D = \{y \in H_{\mathbf{A}} \,|\, \Lambda y = \Lambda\}$ with a maximal lattice Λ in W. In such a case, the left-hand side of (36b) can be given by (17) with $(H,\, \Lambda)$ in place of $(G,\, L)$. Actually $\mathfrak{m}(H,\, H_{\mathbf{A}} \cap D)$ for a general type of D is $\mathfrak{m}(H,\, \Lambda)$ times a certain group index, as will be shown in Theorem 10.

5. Some more comments on the mass

Take G to be $SO^\varphi(V)$ or more generally a reductive algebraic subgroup of $GL(V)$; define $\mathcal{Z}$ as in Section 4. We fix a Haar measure dg on $G_{\mathbf{a}}$ and a measure dw on $\mathcal{Z}$ so that

$$\int_{G_{\mathbf{a}}} f(g(\mathbf{1}))dg = \int_{\mathcal{Z}} f(w)dw \tag{37}$$

for every integrable function f on $\mathcal{Z}$, where $\mathbf{1}$ is the origin of $\mathcal{Z}$ represented by 1. Now we fix a Haar measure on $G_{\mathbf{A}}$ by the condition that the total measure of $G\backslash G_{\mathbf{A}}$ is one. (Recall that G is a discrete subgroup of $G_{\mathbf{A}}$.) Then we have a well defined measure on $G_{\mathbf{h}}$, as $G_{\mathbf{A}} = G_{\mathbf{a}}G_{\mathbf{h}}$. For a measurable subset S of $G_{\mathbf{a}}$, $G_{\mathbf{h}}$, or $\mathcal{Z}$ we denote by $\mathrm{vol}(S)$ the measure of S.

Theorem 9. *Let D be a subgroup of $G_{\mathbf{A}}$ of the form $D = D_0 G_{\mathbf{a}}$ with an open compact subgroup D_0 of $G_{\mathbf{h}}$, and let $\mathit{\Gamma} = G \cap D$. Then*

$$\mathfrak{m}(G,\, D) = \mathrm{vol}(D_0)^{-1}, \tag{38}$$

$$\nu(\mathit{\Gamma}) = \mathrm{vol}(\mathit{\Gamma}\backslash G_{\mathbf{a}}). \tag{39}$$

Proof. The last formula is obvious if $G_{\mathbf{a}}$ is compact, so we assume that $G_{\mathbf{a}}$ is not compact. Let $\mathfrak{F}$ be a fundamental domain for $\mathit{\Gamma}\backslash\mathcal{Z}$ and let $Y = \{g \in G_{\mathbf{a}} \,|\, g(\mathbf{1}) \in \mathfrak{F}\}$. By (37) we have $\mathrm{vol}(\mathfrak{F}) = \mathrm{vol}(Y)$. Now we easily see that $(\mathit{\Gamma} \cap T)\backslash Y$ gives $\mathit{\Gamma}\backslash G_{\mathbf{a}}$, where T is as in (27a), and so $\mathrm{vol}(\mathit{\Gamma}\backslash G_{\mathbf{a}}) = [\mathit{\Gamma} \cap T : 1]^{-1}\mathrm{vol}(Y)$, which proves (39). (To be precise, we have to eliminate nontrivial fixed points of $\mathit{\Gamma}$ from $\mathfrak{F}$ and ignore subsets of measure 0. Alternatively, we can replace $\mathit{\Gamma}$ by a sugroup with no nontrivial fixed points. Then we prove (iii) of the following theorem, which can be done in an elementary way; see [17, Lemma 24.2 (2)].) Next, take $\mathcal{B} \subset G_{\mathbf{h}}$ so that $G_{\mathbf{A}} = \bigsqcup_{a\in\mathcal{B}} GaD$. Then $G\backslash G_{\mathbf{A}} = \bigsqcup_{a\in\mathcal{B}}(G\backslash GaD)$, and $G\backslash GaD$ is represented by $\mathit{\Gamma}^a\backslash aD$, which can be given by $(\mathit{\Gamma}^a\backslash G_{\mathbf{a}}) \times aD_0$. Therefore $\mathrm{vol}(G\backslash GaD) = \mathrm{vol}(\mathit{\Gamma}^a\backslash G_{\mathbf{a}})\mathrm{vol}(D_0)$. We have thus $1 = \mathrm{vol}(G\backslash G_{\mathbf{A}}) = \sum_{a\in\mathcal{B}}\mathrm{vol}(G\backslash GaD) = \sum_{a\in\mathcal{B}}\mathrm{vol}(\mathit{\Gamma}^a\backslash G_{\mathbf{a}})\mathrm{vol}(D_0)$, which combined with (27) and (39) proves (38). □

Theorem 10. *Let D be as above, and let $D' = D'_0 G_{\mathbf{a}}$ with an open compact subgroup D'_0 of $G_{\mathbf{h}}$; put $\mathit{\Gamma} = G \cap D$ and $\mathit{\Gamma}' = G \cap D'$. Then*

(i) *$[\mathit{\Gamma} : \mathit{\Gamma}'] \le [D : D'] < \infty$ if $D' \subset D$.*

(ii) *$[D : D \cap D']\mathfrak{m}(G, D) = [D' : D \cap D']\mathfrak{m}(G, D')$.*

(iii) *$[\mathit{\Gamma} : \mathit{\Gamma} \cap \mathit{\Gamma}']\nu(\mathit{\Gamma}) = [\mathit{\Gamma}' : \mathit{\Gamma} \cap \mathit{\Gamma}']\nu(\mathit{\Gamma}')$.*

(iv) *$\nu(\mathit{\Gamma}) = \nu(\alpha\mathit{\Gamma}\alpha^{-1})$ for every $\alpha \in G$ and $\mathfrak{m}(D) = \mathfrak{m}(xDx^{-1})$ for every $x \in G_{\mathbf{A}}$.*

Proof. If $D' \subset D$, we have $[\mathit{\Gamma} : \mathit{\Gamma}'] = [\mathit{\Gamma}D' : D'] \le [D : D'] = [D_0 : D'_0] < \infty$, as D'_0 is open and D_0 is compact. This proves (i). The remaining three assertions follow immediately from (38) and (39). □

Let us now show that $\mathfrak{m}(S)$ of (31) can be defined independently of the choice of ζ and $\mathit{\Gamma}$. First of all, we easily see that ζ can be replaced by any element of $H\zeta\mathit{\Gamma}$ with the same value of $\nu(\mathit{\Delta}_\zeta)$. Now let $\mathit{\Gamma}' = G \cap D'$ with D' as in Theorem 10 contained in D. Then $h\zeta\mathit{\Gamma} = \bigsqcup_{\alpha\in A} h\zeta\alpha\mathit{\Gamma}$ with $A = \zeta^{-1}\mathit{\Delta}_\zeta\zeta\backslash\mathit{\Gamma}/\mathit{\Gamma}'$. Put $E_\alpha = H \cap \zeta\alpha\mathit{\Gamma}'\alpha^{-1}\zeta^{-1}$. By (iii) above we have

$$(*) \qquad \sum_{\alpha\in A}\nu(E_\alpha)/\nu(\mathit{\Gamma}') = \sum_{\alpha\in A}[\mathit{\Delta}_\zeta : E_\alpha]\nu(\mathit{\Delta}_\zeta)/\nu(\mathit{\Gamma}') = \frac{\nu(\mathit{\Delta}_\zeta)}{\nu(\mathit{\Gamma})[\mathit{\Gamma} : \mathit{\Gamma}']}\sum_{\alpha\in A}[\mathit{\Delta}_\zeta : E_\alpha].$$

We easily see that $\zeta^{-1}\mathit{\Delta}_\zeta\zeta\alpha\mathit{\Gamma}' = \bigsqcup_{\beta\in B_\alpha}\beta\alpha\mathit{\Gamma}'$ with $B_\alpha = \zeta^{-1}\mathit{\Delta}_\zeta\zeta\backslash\zeta^{-1}E_\alpha\zeta$. Thus $\sum_\alpha[\mathit{\Delta}_\zeta : E_\alpha] = \sum_\alpha \#B_\alpha = [\mathit{\Gamma} : \mathit{\Gamma}']$, and so the quantity of $(*)$ equals $\nu(\mathit{\Delta}_\zeta)/\nu(\mathit{\Gamma})$. This proves that $\mathfrak{m}(S)$ defined with respect to $\mathit{\Gamma}'$ gives the same value as (31) as expected.

6. Additional comments on formula (21) and some remarks

Let us now discuss how to obtain (21) and also add various related facts. Assuming $F = \mathbf{Q}$ and φ to be definite, take a $\mathbf{Z}$-lattice L in V and take $\{L_i\}_{i\in I}$ as in (14a). We then put

$$\theta_i(z) = \sum_{x\in L_i} \exp\bigl(2\pi i\varphi[x]\bigr) = \sum_{q\in\mathbf{Q}} \#L_i[q]e^{2\pi iqz}, \quad z \in \mathbf{C},\ \mathrm{Im}(z) > 0, \tag{40}$$

$$f(z) = \Bigl\{\sum_{i\in I}[\varGamma_i : 1]^{-1}\Bigr\}^{-1}\sum_{i\in I}[\varGamma_i : 1]^{-1}\theta_i(z) = \sum_{q\in\mathbf{Q}} b(q)e^{2\pi iqz}, \tag{41}$$

where $\varGamma_i = \varGamma(L_i)$. Then θ_i is a modular form of weight $n/2$; see [15]. Formula (20) shows that $b(q)$, if nonzero, equals $e_\infty \prod_p e_p$.

Theorem 11. (i) *f is an Eisenstein series.*
(ii) *$\theta_i - f$ is a cusp form.*

Proof. For $n > 4$ Siegel proved (i) in [25, Satz 3]; (ii) was also shown in [25, p. 376]. An easier proof of (ii) valid even in the Hilbert modular case is given in [20, Theorem A4.3 (2)]. To prove (i) in general, we first note that

$$f(z) = \int_{G\backslash G_\mathbf{A}} \theta(z,\, g)dg, \qquad \Bigl(\int_{G\backslash G_\mathbf{A}} dg = 1\Bigr), \tag{42}$$

$$\text{where}\quad \theta(z,\, g) = \sum_{x\in Lg^{-1}} \exp\bigl(2\pi i\varphi[x]\bigr) \qquad (g \in G_\mathbf{A}).$$

Indeed, let $D = \bigl\{x \in G_\mathbf{A}\,\big|\, Lx = L\bigr\}$ and $G_\mathbf{A} = \bigsqcup_{i\in I} Ga_iD$. Then we can take La_i^{-1} as L_i. Putting $\varGamma^a = G \cap aDa^{-1}$ as in Section 4, we have $\varGamma^{a_i} = \varGamma_i$. Since $G\backslash G_\mathbf{A} = \bigsqcup_i (G\backslash Ga_iD)$ and $G\backslash GaD$ can be given by $\varGamma^a\backslash aD$ as observed in the proof of Theorem 9, we have

$$\int_{G\backslash G_\mathbf{A}} \theta(z,\, g)dg = \sum_{i\in I}\int_{\varGamma_i\backslash a_iD} \theta(z,\, g)dg.$$

Clearly $\theta(z,\, g) = \theta_i(z)$ if $g \in a_iD$, and so the last sum equals $\sum_i \mathrm{vol}(\varGamma_i\backslash a_iD)\theta_i(z)$ $= \sum_i \mathrm{vol}(D_0)\mathrm{vol}(\varGamma_i\backslash G_\mathbf{a})\theta_i(z)$ for the reason explained in the proof of Theorem 9. This combined with (38) and (39) gives (42). Now by virtue of the Siegel-Weil formula [30] we have, for $n > 4$,

$$\int_{G\backslash G_\mathbf{A}} \theta(z,\, g)dg = \text{an Eisenstein series explicitly depending on}(\varphi,\, L). \tag{43}$$

This proves (i) for $n > 4$. This is true even for $2 \le n \le 4$ by virtue of [11] and [14]; see also the explanation of this point in [19, pp. 86–87]. □

Now there is a technique of expressing each Fourier coefficient of an Eisenstein series as an infinite product of local integrals; see [17], [20], and the author's papers cited there. This gives a proof of the equality $b(q) = e_\infty \prod_p e_p$, with each e_p given as a local integral; for details, see [19]. Thus, as we said, the number of (21) is computable in that sense, but not $\#L_i[q]$ (unless $\#I = 1$). Next, here are two basic facts on an arbitrary elliptic modular form $h(z) = \sum_{q\in\mathbf{Q}} a_q e^{2\pi iqz}$ of weight k, where $0 < k \in 2^{-1}\mathbf{Z}$:

(A) *There is a constant M depending only on h such that $|a_q| \le Mq^k$ for every $q \in \mathbf{Q}, > 0$. Moreover, if h is a cusp form, then M can be taken so that $|a_q| \le Mq^{k/2}$ for every $q \in \mathbf{Q}, > 0$.*

(B) *There exist an Eisenstein series h_0 and a cusp form h_1 such that $h = h_0 + h_1$. Moreover, such h_0 and h_1 are unique for h.*

These are due to Hecke when $k \in \mathbf{Z}$. The proof for an arbitrary $k \in 2^{-1}Z$, even in the Hilbert modular case, can be found in [20, Proposition A6.4] and [16].

Thus the decomposition $\theta_i = f + (\theta_i - f)$ is an expression of type (B); also the estimate given in (A) means that f is "the dominant part" of θ_i. Consequently $b(q)$ gives $\#L_i[q]$ asymptotically.

Let us now add some remarks and a few problems.

(R1) The exact formulas (17) and (21) have been obtained when L is maximal. Now take $\varphi[x] = \sum_{i=1}^{n} x_i^2$. Then the lattice $\mathbf{Z}^n$ is maximal if and only if $n \le 3$, and therefore (21) is not applicable if $n > 3$. However, the problem can be reduced to the case of maximal lattices for such a φ, and so we can give exact formulas for $b(q)$ not only when L is maximal but also when $L = \mathbf{Z}^n$. It is classically known that the genus of $\mathbf{Z}^n$ has class number 1 for $1 \le n \le 8$. It can also be shown that the genus of maximal lattices has class number 1 for $1 \le n \le 9$. Thus, in all such cases we have explicit (and computable) formulas for $\#L[q]$. For details the reader is referred to [21]. Also, we can take, instead of a lattice L, a coset $M = L + y$ with $y \in V$ and define the genus, class, and mass with respect to M. Moreover, we can define the analogues of θ_i and f by taking M in place of L. Then Theorem 11 holds in that case. Formula (20) and what we said about $b(q)$ can be generalized too. The results can be used for the question about the representation of integers as sums of polygonal numbers. For all these, see [23].

(R2) Still with $\varphi[x] = \sum_{i=1}^{n} x_i^2$, let us now explain how to obtain $\#L[q, \mathbf{Z}]$ and $\#L[q, 2^{-1}\mathbf{Z}]$ as stated in Theorem 5. Here L is maximal. For $n \le 9$ formula (36b) shows that $\#L[q, \mathfrak{b}]/\#\mathit{\Gamma}(L) = \mathfrak{m}(H, H_{\mathbf{A}} \cap D)$, provided $L[q, \mathfrak{b}] \ne \emptyset$. Take q to be an odd prime number and $n = 5$, 7, or 9. Then $H_{\mathbf{A}} \cap D$ is the stabilizer of a maximal lattice in W, and so $\mathfrak{m}(H, H_{\mathbf{A}} \cap D)$ is computable by means of (17) with H as G there. Also $L[q] = L[q, \mathbf{Z}] \cup L[q, 2^{-1}\mathbf{Z}]$ if q is a squarefree positive integer. Now the formulas of Theorem 5 can be obtained by combining these facts and using Theorem 10 (ii); for details the reader is referred to [22, Theorem 13.14], where all the values of $A_n(q)$ and $c_n(q)$ are given.

(R3) The determination of $\#\mathbf{Z}^n[q]$ for $\varphi[x] = \sum_{i=1}^{n} x_i^2$ is a subject investigated by many mathematicians. We mention here only the paper [8] by Hardy, in which the problem was treated by the circle method. Also, the introduction of the paper includes a short history of the problem. The case of even n can be handled without difficulties, but for odd n he obtained only $\#(\mathbf{Z}^n)^0[q]$ for $n = 5$ and 7, but not $\#\mathbf{Z}^n[q]$. His idea was all right, but there were nontrivial mistakes, as Stanley pointed out in her paper [29] on $\#(\mathbf{Z}^n)^0[q]$ for $n = 7$. Hardy's own corrections were published in [9]. In his later articles on this topic he cited only [8] and never mentioned [9] or [29].

(R4) There is an old and natural method of treating the sum of three squares. Namely we consider a quaternion algebra $B = \mathbf{Q} + \mathbf{Q}i + \mathbf{Q}j + \mathbf{Q}k$ with the standard Hamilton quaternion units i, j, k. If $0 \ne q = a^2 + b^2 + c^2$ with $a, b, c \in \mathbf{Z}$, then $ai + bj + ck$ generates a subfield of B isomorphic to $\mathbf{Q}(\sqrt{-q}\,)$. For a prime p, B_p is a division algebra if and only if $p = 2$, and so a well known principle says that the prime 2 cannot split in $\mathbf{Q}(\sqrt{-q}\,)$. This is the easiest way to find the condition for the representability of q as a sum of three squares. Moreover, the problem about the number of representations can be reduced to that of counting the embeddings of $\sqrt{-q}$ into a maximal order of B. We can similarly treat some other ternary forms even over an algebraic number field by the same technique. This gives satisfactory results in some special cases, but in general we cannot obtain explicit formulas as good as what is given by (20). We mention here only [5] by Donkar, in which the basic ideas are explained and several references before 1975 are given.

(R5) As we already said, it is a highly nontrivial problem to determine when $L[q,\, \mathfrak{b}] \neq \emptyset$. For instance, in the setting of Theorem 5 we have $L[q,\, 2^{-1}\mathbf{Z}] \neq \emptyset$, but $L[q,\, \mathbf{Z}] = \emptyset$ can happen. Also, as Theorem 6 shows, the expected necessary and sufficient condition is not simple. Still we can ask if there exists a reasonably simple necessary or sufficient condition for $L[q,\, 2^{-1}\mathbf{Z}] \neq \emptyset$.

(R6) At present, formulas (30) and (33) are the best we can say about the problem for an arbitrary $m < n$, though we can add something more when $m = n-1$. If $m = 1$, we have (35), which explains the meaning of "the genus" of h. We naturally ask: can we characterize the set $\mathcal{V} \cap hDy^{-1}$ in a similar way when $m > 1$?

(R7) As shown in Theorem 11 (ii) and explained after the proof, the weighted average of (20) gives an asymptotic value of $\#L[q]$. Is there any analogue of this phenomenon for $\#L[q,\, \mathfrak{b}]$? Namely, does the quantity

$$\left\{\sum_j (\#\Gamma_j)^{-1}\right\}^{-1} \sum_j \#L_j[q,\, \mathfrak{b}]/\#\Gamma_j$$

give the value $\#L[q,\, \mathfrak{b}]$ asymptotically? Here the notation is as in (36b), and j runs over the indices for which $L_j[q,\, \mathfrak{b}] \neq \emptyset$.

Acknowledgments

This article is an expanded version of my Gill Distinguished Lectures at the Department of Mathematics, University of California, Los Angeles, May 17, 19, and 20, 2005. The author thanks the school for giving him the chance to organize the ideas and also for their hospitality during his stay there.

References

[1] P. Bachmann, Die Arithmetik der Quadratischen Formen, Leipzig, Teubner, 1898.

[2] A. Borel, Some finiteness properties of adele groups over number fields, Publ. Math. IHES, No. 16, 1963. MR0202718 (34:2578)

[3] Z. I. Borevich and I. R. Shafarevich, Number Theory, Academic Press, New York and London, 1966. MR0195803 (33:4001)

[4] L. Dirichlet, Vorlesungen über Zahlentheorie, supplement by R. Dedekind, Braunschweig, 1894.

[5] E. N. Donkar, On sums of three integral squares in algebraic number fields, Amer. J. Math. 99 (1977), 1297–1328. MR0460286 (57:280)

[6] M. Eichler, Quadratische Formen und orthogonale Gruppen, Springer, Berlin, 1952; 2nd ed., 1974. MR0351996 (50:4484)

[7] C. F. Gauss, Disquisitiones Arithmeticae; 1801; English translation by A. A. Clarke, Yale Univ. Press, 1966. MR0197380 (33:5545)

[8] G. H. Hardy, On the representation of a number as the sum of any number of squares, and in particular of five, Trans. Amer. Math. Soc. 21 (1920), 255–284. MR1501144

[9] Hardy, Errata, Trans. Amer. Math. Soc. 29 (1927), 845–847. MR1500501

[10] E. Hecke, Vorlesungen über die Theorie der Algebraischen Zahlen, Leipzig, 1923; Chelsea, New York, 1948. MR0352036 (50:4524)

[11] S. Kudla and S. Rallis, On the Weil-Siegel formula, J. Reine Angew. Math. 387 (1988), 1–68. MR0946349 (90e:11059)

[12] Lagrange, Recherches d'Arithmétique, 1773–75, Oeuvres III, 695–758.

[13] Legendre, Recherches d'Analyses Indéterminée, 1785.

[14] S. Rallis, L-functions and the oscillator representation, Lecture Notes in Math., No. 1245, Springer, 1987. MR0887329 (89b:11046)

[15] G. Shimura, On modular forms of half integral weight, Ann. of Math. 97 (1973), 440–481 (= Collected Papers II, 532–573). MR0332663 (48:10989)

[16] G. Shimura, On the Eisenstein series of Hilbert modular groups, Revista Matemática Iberoamericana 1 (1985), 1–42 (= Collected Papers III, 644–685). MR0836282 (87h:11038)

[17] G. Shimura, Euler Products and Eisenstein Series, CBMS Regional Conference Series in Mathematics, No. 93, Amer. Math. Soc., 1997. MR1450866 (98h:11057)

[18] G. Shimura, An exact mass formula for orthogonal groups, Duke Math. J. 97 (1999), 1–66 (= Collected Papers IV, 509–574). MR1681092 (2000a:11073)

[19] G. Shimura, The number of representations of an integer by a quadratic form, Duke Math. J. 100 (1999), 59–92 (= Collected Papers IV, 575–608). MR1714755 (2001f:11057)

[20] G. Shimura, Arithmeticity in the theory of automorphic forms, Mathematical Surveys and Monographs, vol. 82, Amer. Math. Soc., 2000. MR1780262 (2001k:11086)

[21] G. Shimura, The representation of integers as sums of squares, Amer. J. Math. 124 (2002), 1059–1081. MR1925343 (2003i:11049)

[22] G. Shimura, Arithmetic and analytic theories of quadratic forms and Clifford groups, Mathematical Surveys and Monographs, vol. 109, Amer. Math. Soc., 2004. MR2027702 (2004m:11068)

[23] G. Shimura, Inhomogeneous quadratic forms and triangular numbers, Amer. J. Math. 126 (2004), 191–214. MR2033567 (2005a:11047)

[24] G. Shimura, Integer-valued quadratic forms and quadratic Diophantine equations, preprint 2005.

[25] C. L. Siegel, Über die analytische Theorie der quadratischen Formen, Ann. of Math. 36 (1935), 527–606 (= Gesammelte Abhandlungen I, 326–405). MR1503238

[26] C. L. Siegel, Über die analytische Theorie der quadratischen Formen II, Ann. of Math. 37 (1936), 230–263 (= Gesammelte Abhandlungen I, 410–443). MR1503276

[27] C. L. Siegel, Über die Zetafunktionen indefiniter quadratischer Formen II, Math. Zeitschr. 44 (1939), 398–426 (= Gesammelte Abhandlungen II, 68–96). MR1545778

[28] C. L. Siegel, Zur Theorie der quadratischen Formen, Nachr. Akad. Wiss. Göttingen, Math.-phys. Klasse, 1972, Nr. 3, 21–46 (= Gesammelte Abhandlungen IV, 224–249). MR0311578 (47:140)

[29] G. K. Stanley, On the representation of a number as the sum of seven squares, J. London Math. Soc. 2 (1927), 91–96.

[30] A. Weil, Sur la formule de Siegel dans la théorie des groupes classiques, Acta Math. 113 (1965), 1–87 (= Collected Papers III, 71–157). MR0223373 (36:6421)

[31] A. Weil, Number Theory, Birkhäuser, Boston, Basel, Stuttgart, 1984. MR0734177 (85c:01004)

Department of Mathematics, Princeton University, Princeton, NJ 08544-0001