ACTA ARITHMETICA
LXX.4 (1995)

Northcott's theorem on heights
II. The quadratic case

by

WOLFGANG M. SCHMIDT (Boulder, Colo.)

1. Introduction. The distribution of algebraic points in projective space $\mathbb{P}^n(A)$, where A is the field of algebraic numbers, is best described in terms of their height. When K is an algebraic number field and P a point in $\mathbb{P}^n(K)$, let $H_K(P)$ be the multiplicative field height as defined in [8], [11], [12], [13] or [14]. When $P = (\alpha_0 : \ldots : \alpha_n)$ lies in $\mathbb{P}^n(A)$, let $K = \mathbb{Q}(P)$ be the field obtained from $\mathbb{Q}$ by adjoining the ratios α_i/α_j $(0 \le i, j \le n; \alpha_j \ne 0)$, and set $\mathcal{H}(P) = H_K(P)$. Note that $\mathcal{H}(P)$ is the dth power of the absolute height $H(P)$ as defined in the literature, where $d = \deg \mathbb{Q}(P)$.

Given a field K, let $N(K, n, X)$ be the number of points $P \in \mathbb{P}^n(K)$ with $H_K(P) \le X$. Given d, let $\mathcal{N}(d, n, X)$ be the number of points $P \in \mathbb{P}^n(A)$ with $\deg \mathbb{Q}(P) = d$ and $\mathcal{H}(P) \le X$.

Schanuel [11] had proved an asymptotic formula

$$N(K,n,X) = c_1(K,n)X^{n+1} + \begin{cases} O(X \log X) & \text{when } d = n = 1, \\ O_{Kn}(X^{n+1-(1/d)}) & \text{otherwise.} \end{cases} \tag{1.1}$$

The constant $c_1(K,n)$ was explicitly given by Schanuel; like all constants in this paper, it is positive. Further $d = \deg K$, and the constant implicit in $O_{Kn}(\ldots)$ depends on K and n only. On the other hand, the quantity $\mathcal{N}(d,n,X)$ is finite by Northcott's Theorem [10] but its estimation is more difficult. In the first part [13] of the present series we showed that for given d, n and $X > X_0(d,n)$,

$$c_2(d,n)X^{\max(d+1,n+1)} < \mathcal{N}(d,n,X) < c_3(d,n)X^{d+n}. \tag{1.2}$$

(In fact, we dealt with the more general situation where the condition $[\mathbb{Q}(P) : \mathbb{Q}] = d$ was replaced by $[k(P) : k] = d$, where k is a given algebraic number field.) In the present paper we will obtain more information in the case when $d = 2$.

Supported in part by NSF grant DMS-9108581.

Let $N'(K,n,X)$ be the number of points $P \in \mathbb{P}^n(K)$ with $\mathbb{Q}(P) = K$ and $H_K(P) \le X$. (Note that $\mathcal{H}(P) = H_K(P)$ for such points.) It is easily seen that $N'(K,n,X)$ satisfies the same asymptotic formula (1.1) as $N(K,n,X)$. Since

$$\mathcal{N}(d,n,X) = \sum_K N'(K,n,X), \tag{1.3}$$

where the sum is over all number fields K of degree d, it is tempting to take the sum over the right hand side of (1.1). However, in order to do so, one needs to know the implied constants in $O_{Kn}(\ldots)$. (One also needs information on the collection of all fields of given degree d; this information is readily available only for $d = 2$, when the fields are parametrized by their discriminant.)

In the present paper we will obtain a more precise version of (1.1) for quadratic fields K. Our work will also lead to a more explicit form of a classical asymptotic formula of Dirichlet on ideals with bounded norm in a given quadratic number field. (This formula was later extended to arbitrary fields by Dedekind.)

Let K be a quadratic number field with discriminant Δ, class number h, and with w roots of unity. In the case when K is real, so that $\Delta > 0$, let $\varepsilon > 1$ be the fundamental unit. Set

$$R = \begin{cases} 1 & \text{when } \Delta < 0, \\ \log\varepsilon & \text{when } \Delta > 0, \end{cases} \tag{1.4}$$

$$\lambda = \begin{cases} 2\pi & \text{when } \Delta < 0, \\ 4 & \text{when } \Delta > 0. \end{cases} \tag{1.5}$$

Finally, for $X > 0$, let $Z(K,X)$ be the number of nonzero integral ideals $\mathfrak{a}$ in K with norm $\mathfrak{N}(\mathfrak{a}) \le X$. Dirichlet's asymptotic formula says that when K is fixed and $X \to \infty$, then

$$Z(K,X) \sim \frac{\lambda h R}{w|\Delta|^{1/2}} X.$$

It is easily seen that the error term here is $O_K(X^{1/2})$. In fact, the exponent $1/2$ can be reduced, but we will not be concerned with this here. Rather we will estimate the implied constant in O_K.

THEOREM 1.

$$Z(K,X) = \frac{\lambda h R}{w|\Delta|^{1/2}} X + O((XhR\log^+(hR))^{1/2}).$$

Here the implied constant in $O(\ldots)$ is absolute, and $\log^+ x = \max(1, \log x)$. In fact, all the constants which will occur in the sequel in $O(\ldots)$ or in $\ll$ will depend only on occasional parameters n, m, l, σ, α, δ, but will be independent of the field K.

Schanuel's constant $c_1(K,n)$ occurring in (1.1), in the case of a quadratic field K, is given by

$$c_1(K,n) = \frac{\nu hR}{w\zeta_K(n+1)}\left(\frac{\lambda}{|\Delta|^{1/2}}\right)^{n+1}, \tag{1.6}$$

where ζ_K is the Dedekind zeta function of K and where

$$\nu = \begin{cases} 1 & \text{when } \Delta < 0, \\ n+1 & \text{when } \Delta > 0. \end{cases} \tag{1.7}$$

We now introduce

$$c_1^*(K,n) = |\Delta|^{-n/2}(hR\log^+(hR))^{1/2}. \tag{1.8}$$

Theorem 2. *For a quadratic field* K,

$$N'(K,n,X) = c_1(K,n)X^{n+1} + O(c_1^*(K,n)X^{n+(1/2)}).$$

This leads also to an estimate for $N(K,n,X)$. For the points counted by $N(K,n,X)$ but not by $N'(K,n,X)$ are points P with $\mathbb{Q}(P) = \mathbb{Q}$, i.e., with $P \in \mathbb{P}^n(\mathbb{Q})$ and $H_K(P) = H_{\mathbb{Q}}(P)^2 \le X$. Therefore

$$N(K,n,X) = N'(K,n,X) + N(\mathbb{Q},n,X^{1/2}) = N'(K,n,X) + O(X^{(n+1)/2}).$$

Write

$$\mathcal{N}(2,n,X) = \mathcal{N}^-(2,n,X) + \mathcal{N}^+(2,n,X),$$

where $\mathcal{N}^-(2,n,X)$, $\mathcal{N}^+(2,n,X)$ is the number of points $P \in \mathbb{P}^n(A)$ with $\deg \mathbb{Q}(P) = 2$ and $\mathcal{H}(P) \le X$, and where the discriminant $\Delta(\mathbb{Q}(P))$ is < 0 or > 0, respectively.

Theorem 3. *When* $n \ge 3$, *then*

$$\mathcal{N}^{\pm}(2,n,X) = c_5^{\pm}(n)X^{n+1} + O(X^{n+(1/2)})$$

with certain constants $c_5^+(n)$, $c_5^-(n)$ *defined in Section* 8. *Here and below*, *the relations hold with superscript* $+$ *throughout*, *or superscript* $-$ *throughout. Further when* $n = 2$,

$$\mathcal{N}^{\pm}(2,2,X) = c_6^{\pm}X^3\log X + O(X^3\sqrt{\log X})$$

with

$$c_6^+ = \frac{48}{\zeta(3)^2}, \qquad c_6^- = \frac{4\pi^2}{\zeta(3)^2},$$

and when $n = 1$,

$$\mathcal{N}^{\pm}(2,1,X) = c_7^{\pm}X^3 + O(X^2\log X)$$

with

$$c_7^+ = \frac{40}{9\zeta(3)}, \qquad c_7^- = \frac{32}{9\zeta(3)}.$$

The theorem shows that for $d = 2$, the lower bounds in (1.2) are near the truth. We expect this to be true in general. In fact Gao Xia will soon publish results for $d > 2$.

Next, we consider nonzero quadratic forms

$$f(x_0, \ldots, x_n) = \sum_{0 \le i \le j \le n} a_{ij} x_i x_j \tag{1.9}$$

with rational coefficients. The form is called *decomposable* if it is the product of two linear forms with algebraic coefficients. When f is decomposable, say $f = ll'$ with $l(\boldsymbol{x}) = \sum_{i=0}^{n} \alpha_i x_i$, $l'(\boldsymbol{x}) = \sum_{i=0}^{n} \alpha'_i x_i$, then by unique factorization the (unordered) pair of points $P = (\alpha_0 : \ldots : \alpha_n)$, $P' = (\alpha'_0 : \ldots : \alpha'_n)$ in $\mathbb{P}^n(A)$ is uniquely determined by f. We have $\mathbb{Q}(P) = \mathbb{Q}(P') = K(f)$, say, with $K(f)$ either a quadratic or the rational field.

Let $\mathcal{Z}(n, X)$ be the number of decomposable quadratic forms with coefficients $a_{ij} \in \mathbb{Z}$ having $|a_{ij}| \le X$ $(0 \le i \le j \le n)$. We write

$$\mathcal{Z}(n, X) = \mathcal{Z}^-(n, X) + \mathcal{Z}^+(n, X) + \mathcal{Z}^0(n, X),$$

where $\mathcal{Z}^-$, $\mathcal{Z}^+$, $\mathcal{Z}^0$ respectively count only those forms for which $K(f)$ is imaginary quadratic, real quadratic, or the rational field. Since every form in 1 or 2 variables is decomposable, the interesting cases are when $n \ge 2$.

Theorem 4. *We have*

$$\mathcal{Z}^{\pm}(2, X) = c_8^{\pm}(2) X^3 \log X + O(X^3 \sqrt{\log X}),$$
$$\mathcal{Z}^{\pm}(n, X) = c_8^{\pm}(n) X^{n+1} + O(X^{n+(1/2)}) \quad \textit{when } n \ge 3.$$

On the other hand, *for* $n \ge 2$,

$$\mathcal{Z}^0(n, X) = c_8^0(n) X^{n+1} \log X + O(X^{n+1}).$$

In particular, $\mathcal{Z}(n, X) \sim c_9(n) X^{n+1} \log X$ for $n \ge 2$. It is somewhat surprising that when $n \ge 3$, the number $\mathcal{Z}^0(n, X)$ is of larger order of magnitude than $\mathcal{Z}^-(n, X)$ or $\mathcal{Z}^+(n, X)$. Our proof will imply fairly explicit values for the constants $c_8^{\pm}(n)$.

The form f could also be written as

$$f = \sum_{i,j=0}^{n} b_{ij} x_i x_j$$

with $b_{ij} = b_{ji}$. The form f is decomposable precisely when the symmetric matrix (b_{ij}) has rank ≤ 2. Therefore $\mathcal{Z}(n, X)$ may be interpreted as the number of symmetric $(n+1) \times (n+1)$-matrices with rank ≤ 2 such that $b_{ii} \in \mathbb{Z}$, $|b_{ii}| \le X$, and $2b_{ij} \in \mathbb{Z}$, $2|b_{ij}| \le X$ for $i \ne j$. Of particular interest is the number $\mathcal{Z}(2, X)$, which counts symmetric 3×3-matrices. By a slight generalization of our method it would be possible to obtain a complete analog of Theorem 4 for the number $\mathcal{Z}_1(n,X) = \mathcal{Z}_1^-(n,X) + \mathcal{Z}_1^+(n,X) + \mathcal{Z}_1^0(n,X)$, say, where $\mathcal{Z}_1(n,X)$ is the number of symmetric matrices (b_{ij}) of rank ≤ 2 and order $n+1$ with $b_{ij} \in \mathbb{Z}$, $|b_{ij}| \le X$ $(0 \le i,j \le n)$. Many other variations of Theorem 4 could be given.

For the number $\mathcal{Z}_2(n,X)$ of singular $(n+1)\times(n+1)$-matrices (b_{ij}) (not necessarily symmetric) with $b_{ij} \in \mathbb{Z}$, $|b_{ij}| \le X$, Katznelson [7] gave an asymptotic formula $\mathcal{Z}_2(n,X) \sim c_{10}(n)X^{n^2+n}\log X$, so that in particular $\mathcal{Z}_2(2,X) \sim c_{10}(3)X^3\log X$.

There are two directions in which one could try to generalize Theorem 4. On the one hand, one could consider decomposable forms of degree d (rather than $d = 2$); this leads essentially to questions (formulated at the beginning) on heights of points of degree d. On the other hand, one could consider symmetric matrices of rank $\le d$ (1).

In the appendix we will treat certain sums over L-series which will be needed in the proofs of Theorems 3 and 4.

2. The number of lattice points in certain regions. Let Λ be a lattice in $\mathbb{R}^l$ of determinant $\det\Lambda$, and let $\mathcal{S}$ be a compact set in $\mathbb{R}^l$ of volume $V(\mathcal{S})$. Under suitable conditions, the cardinality of $\Lambda\cap\mathcal{S}$ is about $V(\mathcal{S})/\det\Lambda$. To make this precise, one needs information both on Λ and on $\mathcal{S}$. The "shape" of Λ is roughly described by the successive minima $\lambda_1 \le \ldots \le \lambda_l$ of Λ, as defined by Minkowski. Here λ_i is least such that Λ contains i linearly independent points with Euclidean norm $\le \lambda_i$. We have

$$c_{11}(l) \le \lambda_1\ldots\lambda_l/\det\Lambda \le c_{12}(l), \tag{2.1}$$

according to Minkowski. (See, e.g., Cassels [2, Ch. VIII] or Siegel [17, Theorem 16].) $\mathcal{S}$ will be said to be *of class* m if every line intersects $\mathcal{S}$ in the union of at most m intervals and single points, and if the same is true of the projections of $\mathcal{S}$ on any linear subspace. In particular, $\mathcal{S}$ is convex when it is of class 1.

LEMMA 1. *Suppose $\mathcal{S}$ is of class m, and it lies in the compact ball of radius r and center* $\mathbf{0}$. *Let Λ be a lattice, and N the cardinality of $\Lambda\cap\mathcal{S}$. Then if*

$$\lambda_{l-1} \le r, \tag{2.2}$$

we have

$$N = \frac{V(\mathcal{S})}{\det\Lambda} + O\left(\frac{\lambda_l r^{l-1}}{\det\Lambda}\right).$$

(1) Added in proof. For general matrices of fixed rank, see Y. Katznelson, *Integral matrices of fixed rank* (preprint). For symmetric matrices of fixed rank, see A. Eskin and Y. Katznelson, *Singular symmetric matrices*, Duke Math. J., to appear.

The implicit constant in $O(\ldots)$ *depends only on* l, m, *in agreement with the convention made in the introduction.*

Proof. There are independent lattice points $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_l$ with $\boldsymbol{g}_i \in \lambda_i \mathcal{B}$ $(i = 1, \ldots, l)$, where $\mathcal{B}$ is the closed unit ball. In fact (see [2, p. 135, Lemma 8]), there is a basis $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_l$ of Λ with $\boldsymbol{b}_i \in i\lambda_i \mathcal{B}$ $(i = 1, \ldots, l)$. Let τ be the linear map with $\tau(\boldsymbol{b}_i) = \boldsymbol{e}_i$, where $\boldsymbol{e}_i = (0, \ldots, 1, \ldots, 0)$ (with 1 in the ith component). Thus $\tau(\Lambda) = \mathbb{Z}^l$ and $\tau(\mathcal{B}) = \mathcal{E}$, where $\mathcal{E}$ is an ellipsoid of volume $V(\mathcal{E}) = V(\mathcal{B})/\det \Lambda$. Now $\boldsymbol{e}_i \in i\lambda_i \mathcal{E}$, therefore $(i\lambda_i)^{-1}\boldsymbol{e}_i \in \mathcal{E}$ $(i = 1, \ldots, l)$, so that $\mathcal{E}$ has major axes of lengths $a_1 \le \ldots \le a_l$ with $a_i \gg \lambda_{l-i+1}^{-1}$ $(i = 1, \ldots, l)$. Therefore, the orthogonal projection of $\mathcal{E}$ on any i-dimensional subspace has volume

$$\begin{aligned} (2.3) \qquad & \ll a_{l-i+1} \ldots a_l \ll (a_1 \ldots a_{l-i})^{-1} V(\mathcal{E}) \ll \lambda_{i+1} \ldots \lambda_l V(\mathcal{E}) \\ & \ll \lambda_{i+1} \ldots \lambda_l / \det \Lambda. \end{aligned}$$

Now N is the cardinality of $\mathbb{Z}^n \cap \mathcal{T}$ where $\mathcal{T} = \tau(\mathcal{S})$. According to Davenport [3],

$$|N - V(\mathcal{T})| \ll \max_{\mathcal{T}'} V(\mathcal{T}'), \tag{2.4}$$

where the maximum is over the orthogonal projections $\mathcal{T}'$ of $\mathcal{T}$ on the coordinate planes of dimension $< l$, and where the volume of the 0-dimensional projection is understood to be 1. Here we have used the fact that $\mathcal{T}$ is of class m. Note that $V(\mathcal{T}) = V(\mathcal{S})/\det \Lambda$. Moreover, $\mathcal{S} \subset r\mathcal{B}$, therefore $\mathcal{T} \subset r\mathcal{E}$, and any i-dimensional projection $\mathcal{T}_i'$ has

$$V(\mathcal{T}_i') \ll r^i \lambda_{i+1} \ldots \lambda_l / \det \Lambda \le \lambda_l r^{l-1} / \det \Lambda$$

by (2.3), (2.2). The lemma follows.

We now give a variation on Lemma 1 valid in $\mathbb{R}^2$.

Lemma 2. *Suppose* $\mathcal{S} \subset \mathbb{R}^2$ *is of class* m, *and contains the origin. Suppose it lies in the compact disc of radius* r *and center* $\mathbf{0}$. *Let* $\Lambda \subset \mathbb{R}^2$ *be a lattice*, *and* N' *the number of nonzero lattice points in* $\mathcal{S}$. *Then*

$$N' = V(\mathcal{S})/\det \Lambda + O(r/\lambda_1). \tag{2.5}$$

Note that we do not stipulate a condition (2.2).

Proof. When $r \ge \lambda_1$, the assertion follows from the preceding lemma, since $N - N' = 1 \le r/\lambda_1$ in this case. When $r < \lambda_1$, there is no nonzero lattice point in $\mathcal{S}$, so that $N' = 0$. Further $V(\mathcal{S})/\det \Lambda \ll r^2/\lambda_1\lambda_2 < r/\lambda_1$, since $r < \lambda_1 \le \lambda_2$.

Lemma 3. *Let* $\mathcal{S} \subseteq \mathbb{R}^{2n+2}$ *where* $n \ge 1$. *Suppose that* $\mathcal{S}$ *is of class* m *and contained in the compact ball of radius* r *and center* $\mathbf{0}$. *Write points* $\boldsymbol{x} \in \mathbb{R}^{2n+2}$ *as* $\boldsymbol{x} = (\boldsymbol{x}_0, \ldots, \boldsymbol{x}_n)$ *with each* $\boldsymbol{x}_i \in \mathbb{R}^2$. *Let* Λ *be a lattice in* $\mathbb{R}^2$

with minima λ_1, λ_2. *Then the number* N^* *of points* $\boldsymbol{x} \in \mathcal{S}$ *such that each* $\boldsymbol{x}_i \in \Lambda$ $(i = 0, \ldots, n)$, *and* $\boldsymbol{x}_0, \ldots, \boldsymbol{x}_n$ *span* $\mathbb{R}^2$, *has*

$$N^* = \frac{V(\mathcal{S})}{(\det \Lambda)^{n+1}} + O\biggl(\frac{r^{2n+1}}{\lambda_1 (\det \Lambda)^n}\biggr). \tag{2.6}$$

The constant in $O(\ldots)$ *depends only on* n, m.

Proof. Suppose first that

$$\lambda_2 > r. \tag{2.7}$$

Then any points $\boldsymbol{x}_0, \ldots, \boldsymbol{x}_n$ with $(\boldsymbol{x}_0, \ldots, \boldsymbol{x}_n) \in \mathcal{S}$ and $\boldsymbol{x}_i \in \Lambda$ $(i = 0, \ldots, n)$ have Euclidean norm $\le r < \lambda_2$, and therefore are colinear. We obtain $N^* = 0$. The relation (2.6) is valid since

$$V(\mathcal{S})/\det \Lambda \ll r^{2n+2}/\det \Lambda < r^{2n+1}\lambda_2/\det \Lambda \ll r^{2n+1}/\lambda_1$$

by (2.7), (2.1).

Next, suppose that

$$\lambda_2 \le r. \tag{2.8}$$

Let $\Lambda^* = \Lambda \times \ldots \times \Lambda$ in $\mathbb{R}^{2n+2}$. Then $\det \Lambda^* = (\det \Lambda)^{n+1}$ and the successive minima λ_i^* of Λ^* are easily seen to be

$$\lambda_i^* = \begin{cases} \lambda_1 & \text{when } 1 \le i \le n+1, \\ \lambda_2 & \text{when } n+1 < i \le 2n+2. \end{cases}$$

We write

$$N^* = N_1 - N_2,$$

where N_1 is the number of $\boldsymbol{x} = (\boldsymbol{x}_0, \ldots, \boldsymbol{x}_n) \in \Lambda^* \cap \mathcal{S}$, and N_2 is the number of those $(n+1)$-tuples among them for which $\boldsymbol{x}_0, \ldots, \boldsymbol{x}_n$ do not span $\mathbb{R}^2$. We apply Lemma 1 with $l = 2n+2$ and see that

$$N_1 = \frac{V(\mathcal{S})}{(\det \Lambda)^{n+1}} + O\biggl(\frac{\lambda_2 r^{2n+1}}{(\det \Lambda)^{n+1}}\biggr) = \frac{V(\mathcal{S})}{(\det \Lambda)^{n+1}} + O\biggl(\frac{r^{2n+1}}{\lambda_1 (\det \Lambda)^n}\biggr),$$

since $\lambda_{2n+1}^* = \lambda_2 \le r$, and by (2.1). As for N_2, it counts the point $(\mathbf{0}, \ldots, \mathbf{0})$, as well as points $(\boldsymbol{x}_0, \ldots, \boldsymbol{x}_n) \ne (\mathbf{0}, \ldots, \mathbf{0})$ with $\boldsymbol{x}_0, \ldots, \boldsymbol{x}_n$ colinear. For the latter, we lose only a factor $n+1$ if we assume that $\boldsymbol{x}_0 \ne \mathbf{0}$, and $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ are multiples of $\boldsymbol{x}_0$. Now $\boldsymbol{x}_0$ lies in the disc $\mathcal{B} \subset \mathbb{R}^2$ of radius r. By Lemma 1 with $l = 2$, the number of possibilities for $\boldsymbol{x}_0 \ne \mathbf{0}$ is

$$(\pi r^2/\det \Lambda) + O(1 + \lambda_2 r/\det \Lambda) \ll r^2/\det \Lambda$$

by (2.8), and since $r^2 \ge \lambda_1\lambda_2 \gg \det \Lambda$ by (2.1). Each $\boldsymbol{x}_i$ $(i = 1, \ldots, n)$ lies in the segment S of points spanned by $\boldsymbol{x}_0$ having Euclidean norm $\le r$. Since $V(S) = 0$, we see from Lemma 1 that the number of possibilities for each

$\boldsymbol{x}_i$ $(i = 1, \ldots, n)$ is $\ll \lambda_2 r/\det \Lambda$. Thus

$$N_2 \ll 1 + \frac{\lambda_2^n r^{n+2}}{(\det \Lambda)^{n+1}} \ll \frac{\lambda_2 r^{2n+1}}{(\det \Lambda)^{n+1}} \ll \frac{r^{2n+1}}{\lambda_1 (\det \Lambda)^n}$$

by (2.1), (2.8), on noting that

$$1 \ll (\lambda_1 \lambda_2/\det \Lambda)^{n+1} \le (\lambda_2^2/\det \Lambda)^{n+1} \le \lambda_2^n r^{n+2}/(\det \Lambda)^{n+1}.$$

The lemma follows by combining our estimates for N_1 and N_2.

3. Estimates for a given ideal class. The case $\Delta < 0$. Let K be a quadratic number field of discriminant $\Delta < 0$. We may consider K to be embedded in $\mathbb{C}$. With $\alpha \in K$ we associate the point

$$\widehat{\alpha} = (\operatorname{Re} \alpha, \operatorname{Im} \alpha) \in \mathbb{R}^2.$$

As α runs through the integers of K, then $\widehat{\alpha}$ runs through a lattice $\Lambda \subset \mathbb{R}^2$ of determinant $\frac{1}{2}|\Delta|^{1/2}$. As α runs through a nonzero ideal $\mathfrak{a}$ of K, then $\widehat{\alpha}$ runs through a lattice $\Lambda(\mathfrak{a})$ with $\det \Lambda(\mathfrak{a}) = \frac{1}{2}|\Delta|^{1/2}\mathfrak{N}(\mathfrak{a})$. Denote the successive minima of $\Lambda(\mathfrak{a})$ by $\lambda_1(\mathfrak{a})$, $\lambda_2(\mathfrak{a})$.

Let $\mathfrak{C}$ be an ideal class of K. We define $\mathfrak{N}(\mathfrak{C})$ to be the minimum of $\mathfrak{N}(\mathfrak{c})$ over all integral ideals $\mathfrak{c}$ in $\mathfrak{C}$. It is well known that $\mathfrak{N}(\mathfrak{C}) \le |\Delta|^{1/2}$ (see, e.g., Hecke [6, Satz 96]). The ideal class $\overline{\mathfrak{C}}$ consisting of ideals $\overline{\mathfrak{c}}$ with $\mathfrak{c} \in \mathfrak{C}$ (where the bar indicates complex conjugation) is the inverse of $\mathfrak{C}$, so that $\mathfrak{N}(\mathfrak{C}^{-1}) = \mathfrak{N}(\overline{\mathfrak{C}}) = \mathfrak{N}(\mathfrak{C})$.

Now let $\mathfrak{a}$ be an ideal lying in the ideal class $\mathfrak{A}$. When $\alpha \ne 0$ lies in $\mathfrak{a}$, then $(\alpha) = \mathfrak{a}\mathfrak{b}$ with $\mathfrak{b}$ integral in $\mathfrak{A}^{-1}$, so that $|\alpha|^2 = \mathfrak{N}(\alpha) \ge \mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{A}^{-1}) = \mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{A})$, and

$$\lambda_1(\mathfrak{a}) \ge (\mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{A}))^{1/2}. \tag{3.1}$$

Again let $\mathfrak{a}$ be in the class $\mathfrak{A}$, and write $Z_1(\mathfrak{a}, X)$ for the number of nonzero elements $\alpha \in \mathfrak{a}$ with $\mathfrak{N}(\alpha) \le X\mathfrak{N}(\mathfrak{a})$.

Lemma 4.

$$Z_1(\mathfrak{a}, X) = 2\pi X/|\Delta|^{1/2} + O(X^{1/2}/\mathfrak{N}(\mathfrak{A})^{1/2}).$$

Proof. $Z_1(\mathfrak{a}, X)$ is the number of nonzero $\widehat{\alpha} \in \Lambda(\mathfrak{a})$ with $|\widehat{\alpha}|^2 \le X\mathfrak{N}(\mathfrak{a})$. By Lemma 2 with $r = (X\mathfrak{N}(\mathfrak{a}))^{1/2}$,

$$Z_1(\mathfrak{a}, X) = (\pi X \mathfrak{N}(\mathfrak{a})/\det \Lambda(\mathfrak{a})) + O(r/\lambda_1(\mathfrak{a})).$$

Substituting $\det \Lambda(\mathfrak{a}) = \frac{1}{2}|\Delta|^{1/2}\mathfrak{N}(\mathfrak{a})$, the value of r, as well as (3.1), we obtain the desired result.

Let $n > 0$ and write points in $\mathbb{R}^{2n+2}$ as $\widehat{\boldsymbol{\alpha}} = (\widehat{\alpha}_0, \ldots, \widehat{\alpha}_n)$ with each $\widehat{\alpha}_i \in \mathbb{R}^2$. With $\boldsymbol{\alpha} = (\alpha_0, \ldots, \alpha_n)$ in K^{n+1} we associate the point $\widehat{\boldsymbol{\alpha}} = (\widehat{\alpha}_0, \ldots, \widehat{\alpha}_n)$. Let $\mathcal{S}$ be a compact set in $\mathbb{R}^{2n+2}$ contained in the unit ball centered at the origin. Further suppose that $\mathcal{S}$ is of class m as defined in Section 2. For

$t>0$, let $t\mathcal{S}$ be the set of points $t\widehat{\boldsymbol{\alpha}}$ with $\widehat{\boldsymbol{\alpha}}\in\mathcal{S}$. When $\mathfrak{a}$ is a nonzero ideal in K, let $Z_2(\mathfrak{a},\mathcal{S},X)$ be the number of nonzero $\boldsymbol{\alpha}=(\alpha_0,\ldots,\alpha_n)\in K^{n+1}$ with each $\alpha_i\in\mathfrak{a}$, such that $P=(\alpha_0:\ldots:\alpha_n)$ has $\mathbb{Q}(P)=K$, and such that

$$\widehat{\boldsymbol{\alpha}}=(\widehat{\alpha}_0,\ldots,\widehat{\alpha}_n)\in(X\mathfrak{N}(\mathfrak{a}))^{1/2}\mathcal{S}. \tag{3.2}$$

LEMMA 5. *When* $\mathfrak{a}$ *is in the ideal class* $\mathfrak{A}$,

$$Z_2(\mathfrak{a},\mathcal{S},X)=V(\mathcal{S})(2X/|\Delta|^{1/2})^{n+1}+O\biggl(\frac{X^{n+(1/2)}}{|\Delta|^{n/2}\mathfrak{N}(\mathfrak{A})^{1/2}}\biggr).$$

In agreement with the convention made in the introduction, the implied constant in $O(\ldots)$ *depends only on* n, m.

Proof. $Z_2(\mathfrak{a},\mathcal{S},X)$ is the number of $(\widehat{\alpha}_0,\ldots,\widehat{\alpha}_n)$ with (3.2), such that each $\widehat{\alpha}_i\in\Lambda(\mathfrak{a})$, and such that $\widehat{\alpha}_0,\ldots,\widehat{\alpha}_n$ span $\mathbb{R}^2$. We apply Lemma 3 with $\mathcal{S}$ replaced by $(X\mathfrak{N}(\mathfrak{a}))^{1/2}\mathcal{S}$, and with $r=(X\mathfrak{N}(\mathfrak{a}))^{1/2}$. We obtain

$$Z_2(\mathfrak{a},\mathcal{S},X)=V(\mathcal{S})\frac{(X\mathfrak{N}(\mathfrak{a}))^{n+1}}{(\det\Lambda(\mathfrak{a}))^{n+1}}+O\biggl(\frac{(X\mathfrak{N}(\mathfrak{a}))^{n+(1/2)}}{\lambda_1(\mathfrak{a})(\det\Lambda(\mathfrak{a}))^{n}}\biggr).$$

The lemma follows after we substitute $\det\Lambda(\mathfrak{a})=\frac{1}{2}|\Delta|^{1/2}\mathfrak{N}(\mathfrak{a})$ and (3.1).

4. Estimates for a given ideal class. The case $\Delta>0$. Let K be a quadratic number field with discriminant $\Delta>0$. Let ε be the fundamental unit with $\varepsilon>1$, and set $R=\log\varepsilon$. Then $R\gg 1$ with an absolute implied constant. Define t and $u>0$ by

$$t=[R]+1,\qquad \log u=R/t, \tag{4.1}$$

where [ ] denotes the integer part. Then

$$u^t=\varepsilon\quad\text{ and }\quad 1\ll\log u\le 1. \tag{4.2}$$

With $\alpha\in K$ we associate the point

$$\widehat{\alpha}=(\alpha,\alpha')\in\mathbb{R}^2,$$

where α' is the conjugate of α. As α runs through the integers of K, then $\widehat{\alpha}$ runs through a lattice $\Lambda\subset\mathbb{R}^2$ of determinant $\Delta^{1/2}$. As α runs through a nonzero ideal $\mathfrak{a}$, then $\widehat{\alpha}$ runs through a lattice $\Lambda(\mathfrak{a})$ with $\det\Lambda(\mathfrak{a})=\Delta^{1/2}\mathfrak{N}(\mathfrak{a})$.

Let $v=\sqrt{u}$, so that $1\ll\log v$ by (4.2), and

$$v-1\gg 1. \tag{4.3}$$

Let τ be the linear map $\mathbb{R}^2\to\mathbb{R}^2$ with $\tau(\alpha,\alpha')=(v^{-1}\alpha,v\alpha')$. Then $\Lambda(\mathfrak{a},j):=\tau^j\Lambda(\mathfrak{a})$ (for $j\in\mathbb{Z}$) is a lattice with $\det\Lambda(\mathfrak{a},j)=\det\Lambda(\mathfrak{a})=\Delta^{1/2}\mathfrak{N}(\mathfrak{a})$. Its first minimum is given by

$$\lambda_1(\mathfrak{a},j)=\min_{\alpha\in\mathfrak{a}\setminus\{0\}}(v^{-2j}|\alpha|^2+v^{2j}|\alpha'|^2)^{1/2}. \tag{4.4}$$

Given $\boldsymbol{\alpha} = (\alpha_0, \ldots, \alpha_n) \in K^{n+1} \setminus \{\mathbf{0}\}$, set $\boldsymbol{\alpha}' = (\alpha_0', \ldots, \alpha_n')$ and

$$\psi(\boldsymbol{\alpha}) = |\boldsymbol{\alpha}|/|\boldsymbol{\alpha}'|,$$

where $|\boldsymbol{\alpha}| = \max(|\alpha_0|, \ldots, |\alpha_n|)$. After scalar multiplication by ε, we have $\psi(\varepsilon\boldsymbol{\alpha}) = |\varepsilon/\varepsilon'|\psi(\boldsymbol{\alpha}) = \varepsilon^2\psi(\boldsymbol{\alpha})$. There is a unique integer s with $\varepsilon^{-1} < \psi(\varepsilon^s\boldsymbol{\alpha}) \le \varepsilon$. In view of the unit -1, there are exactly two units η such that

$$\varepsilon^{-1} < \psi(\eta\boldsymbol{\alpha}) \le \varepsilon. \tag{4.5}$$

The interval $\varepsilon^{-1} < x \le \varepsilon$ is the disjoint union of the $2t$ intervals $u^{j-1} < x \le u^j$ with $-t < j \le t$.

We now consider the set $S(\mathfrak{a}, j)$ of nonzero $(\alpha_0, \ldots, \alpha_n) \in K^{n+1}$ with $\alpha_i \in \mathfrak{a}$ $(0 \le i \le n)$ and $u^{j-1} < \psi(\boldsymbol{\alpha}) \le u^j$. This set is in 1-1 correspondence with the set $\widehat{S}(\mathfrak{a}, j)$ of points $(\widehat{\alpha}_0, \ldots, \widehat{\alpha}_n) \in \mathbb{R}^{2n+2}$ with $\widehat{\alpha}_i \in \Lambda(\mathfrak{a})$ $(0 \le i \le n)$ and with $u^{j-1} < \psi(\widehat{\boldsymbol{\alpha}}) \le u^j$, where for $\widehat{\boldsymbol{\alpha}} = (\widehat{\alpha}_0, \ldots, \widehat{\alpha}_n) = (\alpha_0, \alpha_0', \ldots, \alpha_n, \alpha_n')$ we set $\psi(\widehat{\boldsymbol{\alpha}}) = |\boldsymbol{\alpha}|/|\boldsymbol{\alpha}'|$ with $\boldsymbol{\alpha} = (\alpha_0, \ldots, \alpha_n)$ and $\boldsymbol{\alpha}' = (\alpha_0', \ldots, \alpha_n')$. Let $\tau^* = \tau \times \ldots \times \tau$ be the map of $\mathbb{R}^{2n+2}$ with $\tau^*(\boldsymbol{\alpha}, \boldsymbol{\alpha}') = (v^{-1}\boldsymbol{\alpha}, v\boldsymbol{\alpha}')$, i.e., $\tau^*(\alpha_0, \alpha_0', \ldots, \alpha_n, \alpha_n') = (v^{-1}\alpha_0, v\alpha_0', \ldots, v^{-1}\alpha_n, v\alpha_n')$. We have $\psi(\tau^*\widehat{\boldsymbol{\alpha}}) = v^{-2}\psi(\widehat{\boldsymbol{\alpha}}) = u^{-1}\psi(\widehat{\boldsymbol{\alpha}})$. Therefore $\widehat{\widehat{S}}(\mathfrak{a}, j) := \tau^{*j}\widehat{S}(\mathfrak{a}, j)$ consists of points $\widehat{\boldsymbol{\alpha}} = (\widehat{\alpha}_0, \ldots, \widehat{\alpha}_n)$ with

$$\widehat{\alpha}_i \in \Lambda(\mathfrak{a}, j) \quad (i = 0, \ldots, n) \qquad \text{and} \qquad u^{-1} < \psi(\widehat{\boldsymbol{\alpha}}) \le 1.$$

Now let $n = 0$, let $\mathfrak{a}$ be a nonzero ideal, and $-t < j \le t$. Write $Z_1(\mathfrak{a}, j, X)$ for the number of nonzero $\alpha \in \mathfrak{A}$ with $\alpha \in \mathfrak{a}$, $|\alpha\alpha'| \le X\mathfrak{N}(\mathfrak{a})$ and $u^{j-1} < \psi(\alpha) \le u^j$.

Lemma 6.

$$Z_1(\mathfrak{a}, j, X) = (2RX/t\Delta^{1/2}) + O(X^{1/2}\mathfrak{N}(\mathfrak{a})^{1/2}/\lambda_1(\mathfrak{a}, j)).$$

Proof. The set of $\widehat{\alpha} = (\alpha, \alpha') \in \mathbb{R}^2$ with $|\alpha\alpha'| \le X\mathfrak{N}(\mathfrak{a})$ is invariant under τ. Therefore $Z_1(\mathfrak{a}, j, X)$ is the number of $\widehat{\alpha} \in \Lambda(\mathfrak{a}, j)$ with

$$0 < |\alpha\alpha'| \le X\mathfrak{N}(\mathfrak{a}) \qquad \text{and} \qquad u^{-1} < \psi(\widehat{\alpha}) \le 1.$$

These two inequalities define a set $\mathcal{S}$ in $\mathbb{R}^2$. For $\widehat{\alpha} \in \mathcal{S}$, we have $|\alpha| \le |\alpha'| < u|\alpha|$, so that both $|\alpha|, |\alpha'| < (uX\mathfrak{N}(\mathfrak{a}))^{1/2}$, and $\mathcal{S}$ is contained in a disc of radius $r \ll (X\mathfrak{N}(\mathfrak{a}))^{1/2}$. Further $\mathcal{S}$ is of some class $m \ll 1$ (in fact $m = 2$). Although $\mathcal{S}$ is not closed, it is easily seen that Lemma 2 still applies, and we get

$$Z_1(\mathfrak{a}, j, X) = (V(\mathcal{S})/\det\Lambda(\mathfrak{a}, j)) + O(r/\lambda_1(\mathfrak{a}, j)).$$

Since $\det\Lambda(\mathfrak{a}, j) = \Delta^{1/2}\mathfrak{N}(\mathfrak{a})$, and since, as is seen by an easy calculation, $V(\mathcal{S}) = 2X\mathfrak{N}(\mathfrak{a})\log u = 2XR\mathfrak{N}(\mathfrak{a})/t$, the lemma follows.

Let $n > 0$ and write points in $\mathbb{R}^{2n+2}$ as $\widehat{\boldsymbol{\alpha}} = (\widehat{\alpha}_0, \ldots, \widehat{\alpha}_n)$ where each $\widehat{\alpha}_i = (\alpha_i, \alpha_i') \in \mathbb{R}^2$, or else as $\widehat{\boldsymbol{\alpha}} = (\boldsymbol{\alpha}, \boldsymbol{\alpha}')$ with $\boldsymbol{\alpha} = (\alpha_0, \ldots, \alpha_n)$, $\boldsymbol{\alpha}' = (\alpha_0', \ldots, \alpha_n')$. With $\boldsymbol{\alpha} = (\alpha_0, \ldots, \alpha_n) \in K^{n+1}$ we associate the point $\widehat{\boldsymbol{\alpha}} =$

$(\widehat{\alpha}_0,\ldots,\widehat{\alpha}_n)$. Let $\mathcal{S}$ be a closed set in $\mathbb{R}^{2n+2}$ such that the points $\widehat{\boldsymbol{\alpha}} = (\boldsymbol{\alpha},\boldsymbol{\alpha}')$ in $\mathcal{S}$ have $|\boldsymbol{\alpha}|\,|\boldsymbol{\alpha}'|\le 2$, and that $\mathcal{S}$ is invariant under transformations $(\boldsymbol{\alpha},\boldsymbol{\alpha}')\mapsto(t^{-1}\boldsymbol{\alpha},t\boldsymbol{\alpha}')$ with $t>0$. For $x>1$ let $\mathcal{S}(x)$ be the intersection of $\mathcal{S}$ with $x^{-1}<\psi(\widehat{\boldsymbol{\alpha}})\le 1$. Points $\widehat{\boldsymbol{\alpha}}\in\mathcal{S}(x)$ have $|\boldsymbol{\alpha}|^2\le 2$, $|\boldsymbol{\alpha}'|^2\le 2x$, so that $\mathcal{S}(x)$ lies in a ball of radius $r\ll x^{1/2}$. Let $V(\mathcal{S}(x))$ be the volume of $\mathcal{S}(x)$; by the invariance property of $\mathcal{S}$ we have $V(\mathcal{S}(x))=V(\mathcal{S}(e))\log x$. We will finally suppose that the closure of $\mathcal{S}(x)$ is of class m.

For a nonzero ideal $\mathfrak{a}$ and for $-t<j\le t$, let $Z_2(\mathfrak{a},j,\mathcal{S},X)$ be the number of $\boldsymbol{\alpha}=(\alpha_0,\ldots,\alpha_n)$ with $\alpha_i\in\mathfrak{a}$ $(i=0,\ldots,n)$ such that $P=(\alpha_0:\ldots:\alpha_n)$ has $\mathbb{Q}(P)=K$, and such that

$$\widehat{\boldsymbol{\alpha}}\in(X\mathfrak{N}(\mathfrak{a}))^{1/2}\mathcal{S}\quad\text{and}\quad u^{j-1}<\psi(\boldsymbol{\alpha})\le u^j.$$

LEMMA 7.

$$Z_2(\mathfrak{a},j,\mathcal{S},X)=\frac{RV(\mathcal{S}(e))}{t}\left(\frac{X}{\Delta^{1/2}}\right)^{n+1}+O\left(\frac{X^{n+(1/2)}\mathfrak{N}(\mathfrak{a})^{1/2}}{\Delta^{n/2}\lambda_1(\mathfrak{a},j)}\right).$$

Proof. By what we have seen above, $Z_2(\mathfrak{a},j,\mathcal{S},X)$ is the same as the number of points $\widehat{\boldsymbol{\alpha}}=(\widehat{\alpha}_0,\ldots,\widehat{\alpha}_n)$ in $\Lambda(\mathfrak{a},j)\times\ldots\times\Lambda(\mathfrak{a},j)$ such that $\widehat{\alpha}_0,\ldots,\widehat{\alpha}_n$ span $\mathbb{R}^2$, and which lie in the set $\mathcal{S}'$ defined by

$$(\widehat{\alpha}_0,\ldots,\widehat{\alpha}_n)\in(X\mathfrak{N}(\mathfrak{a}))^{1/2}\mathcal{S}\quad\text{and}\quad u^{-1}<\psi(\widehat{\boldsymbol{\alpha}})\le 1.$$

$\mathcal{S}'$ lies in a ball of radius $r\ll(X\mathfrak{N}(\mathfrak{a}))^{1/2}$ and has volume $V(\mathcal{S}')=(X\mathfrak{N}(\mathfrak{a}))^{n+1}(\log u)V(\mathcal{S}(e))$. Lemma 3 gives

$$Z_2(\mathfrak{a},j,\mathcal{S},X)=\frac{V(\mathcal{S}')}{(\det\Lambda(\mathfrak{a},j))^{n+1}}+O\left(\frac{r^{2n+1}}{(\det\Lambda(\mathfrak{a},j))^n\lambda_1(\mathfrak{a},j)}\right).$$

If we substitute our value for $V(\mathcal{S}')$ and $\det\Lambda(\mathfrak{a},j)=\Delta^{1/2}\mathfrak{N}(\mathfrak{a})$, as well as the estimate for r, and the relation $\log u=R/t$ from (4.1), we obtain the assertion of the lemma.

Let $\mathfrak{C}$ be an ideal class. Let $\mathfrak{c}_1,\mathfrak{c}_2,\ldots$ be the integral ideals in $\mathfrak{C}$ ordered so that $\mathfrak{N}(\mathfrak{c}_1)\le\mathfrak{N}(\mathfrak{c}_2)\le\ldots$ We set

$$\mathfrak{N}(\mathfrak{C})=\Big(\sum_{j=1}^{2t}\mathfrak{N}(\mathfrak{c}_j)^{-1/2}\Big)^{-2}. \tag{4.6}$$

This definition differs from the one when $\Delta<0$. It is easily seen that we still have $\mathfrak{N}(\mathfrak{C}^{-1})=\mathfrak{N}(\overline{\mathfrak{C}})=\mathfrak{N}(\mathfrak{C})$.

LEMMA 8. *Let $\mathfrak{a}$ lie in the ideal class $\mathfrak{A}$. Then*

$$\sum_{j=1-t}^{t}1/\lambda_1(\mathfrak{a},j)\ll(\mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{A}))^{-1/2}. \tag{4.7}$$

This estimate takes the place of (3.1) in the case $\Delta<0$.

P r o o f. Define $\mu_1(\mathfrak{a}, j)$ as the minimum of $\max(v^{-j}|\alpha|, v^j|\alpha'|)$ for nonzero $\alpha \in \mathfrak{a}$. Since $\lambda_1(\mathfrak{a}, j) \geq \mu_1(\mathfrak{a}, j)$, it will suffice to estimate the sum (4.7) with μ_1 in place of λ_1. Pick $\alpha = \alpha(\mathfrak{a}, j)$ with

$$\mu_1(\mathfrak{a}, j) = \max(v^{-j}|\alpha|, v^j|\alpha'|).$$

We claim that for $1 - t \leq j \leq t$,

$$\varepsilon^{-2} < \psi(\alpha(\mathfrak{a}, j)) \leq \varepsilon^2. \tag{4.8}$$

For if, say, $\psi(\alpha) > \varepsilon^2$, then

$$v^{-j}|\alpha| > v^{-j}\varepsilon^2|\alpha'| \geq v^j|(\varepsilon^{-1}\alpha)'|,$$

since $\varepsilon^2 v^{-2j} \geq \varepsilon^2 v^{-2t} = \varepsilon = |(\varepsilon^{-1})'|$. Therefore

$$\max(v^{-j}|\alpha|, v^j|\alpha'|) \geq v^{-j}|\alpha| > \max(v^{-j}|\varepsilon^{-1}\alpha|, v^j|(\varepsilon^{-1}\alpha)'|).$$

By the minimal property of $\alpha(j, \mathfrak{a})$, this cannot happen for $\alpha = \alpha(j, \mathfrak{a})$. Therefore $\psi(\alpha(\mathfrak{a}, j)) \leq \varepsilon^2$. The lower bound in (4.8) is proved similarly.

Let $\alpha \in \mathfrak{a}$ be given with $\varepsilon^{-2} < \psi(\alpha) \leq \varepsilon^2$. We consider the sum

$$\sum_{\substack{j \\ \alpha(\mathfrak{a}, j) = \alpha}} (\mu_1(\mathfrak{a}, j))^{-1} \leq \sum_{j \in \mathbb{Z}} \min(v^j|\alpha|^{-1}, v^{-j}|\alpha'|^{-1}).$$

Here $|\alpha| = v^\xi|\mathfrak{N}(\alpha)|^{1/2}$, $|\alpha'| = v^{-\xi}|\mathfrak{N}(\alpha)|^{1/2}$ for some ξ, so that the last sum becomes

$$\begin{aligned} |\mathfrak{N}(\alpha)|^{-1/2} \sum_{j \in \mathbb{Z}} \min(v^{j-\xi}, v^{\xi-j}) &\leq |\mathfrak{N}(\alpha)|^{-1/2} \cdot 2\sum_{j=0}^{\infty} v^{-j} \\ &= (2v/(v-1))|\mathfrak{N}(\alpha)|^{-1/2} \ll |\mathfrak{N}(\alpha)|^{-1/2}, \end{aligned}$$

since $v - 1 \gg 1$ by (4.3).

Suppose s distinct numbers $\alpha_1, \ldots, \alpha_s$ occur among the $\alpha(\mathfrak{a}, j)$ where $-t < j \leq t$, so that clearly $s \leq 2t$. Then

$$\sum_{j=1-t}^{t} \mu_1(\mathfrak{a}, j)^{-1} \ll \sum_{j=1}^{s} |\mathfrak{N}(\alpha_j)|^{-1/2}.$$

We have $(\alpha_j) = \mathfrak{a}\mathfrak{b}_j$ where $\mathfrak{b}_j$ is integral in $\mathfrak{A}^{-1}$. On the other hand, given $\mathfrak{b} \in \mathfrak{A}^{-1}$, there are precisely 4 elements α with $(\alpha) = \mathfrak{a}\mathfrak{b}$ and with $\varepsilon^{-2} < \psi(\alpha) \leq \varepsilon^2$, because $\psi(\pm\varepsilon^s\alpha) = \varepsilon^{2s}\psi(\alpha)$. Therefore, with certain distinct $\mathfrak{b}_1, \ldots, \mathfrak{b}_{2t}$ in $\mathfrak{A}^{-1}$, the sum in (4.7) is

$$\ll \mathfrak{N}(\mathfrak{a})^{-1/2} \sum_{j=1}^{2t} \mathfrak{N}(\mathfrak{b}_j)^{-1/2} \leq \mathfrak{N}(\mathfrak{a})^{-1/2}\mathfrak{N}(\mathfrak{A}^{-1})^{-1/2} = (\mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{A}))^{-1/2},$$

by the definition (4.6).

By (4.2), by taking the sum over j, $-t < j \le t$, in Lemmas 6, 7, and using Lemma 8, we immediately get the next two lemmas.

LEMMA 9. *Let* $\mathfrak{a}$ *be an ideal in the class* $\mathfrak{A}$, *and* $Z_1(\mathfrak{a}, X)$ *the number of nonzero* $\alpha \in \mathfrak{a}$ *with* $|\alpha\alpha'| \le X\mathfrak{N}(\mathfrak{a})$ *and* $\varepsilon^{-1} < \psi(\alpha) \le \varepsilon$. *Then*

$$Z_1(\mathfrak{a}, X) = 4RX/\Delta^{1/2} + O(X^{1/2}/\mathfrak{N}(\mathfrak{A})^{1/2}).$$

LEMMA 10. *Let* $n > 0$, $\mathcal{S}$ *a set in* $\mathbb{R}^{2n+2}$ *as in Lemma* 7, *and* $\mathfrak{a}$ *an ideal in the class* $\mathfrak{A}$. *Let* $Z_2(\mathfrak{a}, \mathcal{S}, X)$ *be the number of* $\boldsymbol{\alpha} = (\alpha_0, \ldots, \alpha_n)$ *with each* $\alpha_i \in \mathfrak{a}$, *with* $P = (\alpha_0 : \ldots : \alpha_n)$ *having* $\mathbb{Q}(P) = K$, *and with*

$$\widehat{\boldsymbol{\alpha}} \in (X\mathfrak{N}(\mathfrak{a}))^{1/2}\mathcal{S} \quad \text{and} \quad \varepsilon^{-1} < \psi(\boldsymbol{\alpha}) \le \varepsilon.$$

Then

$$Z_2(\mathfrak{a}, \mathcal{S}, X) = 2RV(\mathcal{S}(e))(X/\Delta^{1/2})^{n+1} + O(X^{n+(1/2)}\Delta^{-n/2}\mathfrak{N}(\mathfrak{A})^{-1/2}).$$

5. Proof of Theorem 1. Lemmas 4 and 9 may be combined to give

$$Z_1(\mathfrak{a}, X) = \lambda RX/|\Delta|^{1/2} + O(X^{1/2}/\mathfrak{N}(\mathfrak{A})^{1/2}), \tag{5.1}$$

where R, λ are given by (1.4), (1.5). Note that the definitions of $Z_1(\mathfrak{a}, X)$ and $\mathfrak{N}(\mathfrak{A})$ are somewhat different when $\Delta < 0$ and when $\Delta > 0$.

LEMMA 11. *Let* $\mathfrak{C}$ *be an ideal class*, *and define* $Z_3(\mathfrak{C}, X)$ *to be the number of integral ideals* $\mathfrak{c} \in \mathfrak{C}$ *with* $\mathfrak{N}(\mathfrak{c}) \le X$. *Then*

$$Z_3(\mathfrak{C}, X) = \lambda RX/(w\Delta^{1/2}) + O(X^{1/2}/\mathfrak{N}(\mathfrak{C})^{1/2}), \tag{5.2}$$

where w *is the number of roots of* 1 *of the underlying quadratic number field* K.

Proof. Let $\mathfrak{A} = \mathfrak{C}^{-1}$ and fix $\mathfrak{a}$ in $\mathfrak{A}$. When $\mathfrak{c} \in \mathfrak{C}$ with $\mathfrak{N}(\mathfrak{c}) \le X$, then $\mathfrak{ac}$ is a principal ideal (α) with $\alpha \in \mathfrak{a}$, $\alpha \ne 0$, and $|\mathfrak{N}(\alpha)| \le X\mathfrak{N}(\mathfrak{a})$. Conversely, when $\alpha \in \mathfrak{a}$, $\alpha \ne 0$ and $|\mathfrak{N}(\alpha)| \le X\mathfrak{N}(\mathfrak{a})$, then $(\alpha) = \mathfrak{ac}$ with integral $\mathfrak{c} \in \mathfrak{C}$ having $\mathfrak{N}(\mathfrak{c}) \le X$.

If $\Delta < 0$, then α is determined by $\mathfrak{c}$ up to the w roots of 1. Thus Lemma 11 follows from Lemma 4 and the definition of $Z_1(\mathfrak{a}, X)$. When $\Delta > 0$, we may pick α with $\varepsilon^{-1} < \psi(\alpha) \le \varepsilon$, and this will determine α up to multiplication by ± 1, so that we will have $w = 2$ choices for α. Now Lemma 11 follows from Lemma 9 and the definition of $Z_1(\mathfrak{a}, X)$ in the case $\Delta > 0$.

The proof of Theorem 1 is now easily completed by taking the sum over the ideal classes in (5.2). All that is needed is the estimate

$$\sum_{\mathfrak{C}} \mathfrak{N}(\mathfrak{C})^{-1/2} \ll (hR\log^+ hR)^{1/2}. \tag{5.3}$$

When $\Delta < 0$, the sum on the left here is over h terms $\mathfrak{N}(\mathfrak{c}_i)^{-1/2}$, with distinct nonzero integral ideals $\mathfrak{c}_i$. We may suppose that $\mathfrak{N}(\mathfrak{c}_1) \le \ldots \le \mathfrak{N}(\mathfrak{c}_h)$. The number of integral ideals $\mathfrak{c}$ with $\mathfrak{N}(\mathfrak{c}) = u$ is at most $\tau(u)$, the number of positive divisors of u. Since

$$\sum_{u=1}^{x} \tau(u) \sim x \log x$$

(see [5, Theorem 315]), we may conclude that $\mathfrak{N}(\mathfrak{c}_i) \gg i/\log^+ i$. Therefore

$$\sum_{\mathfrak{C}} \mathfrak{N}(\mathfrak{C})^{-1/2} = \sum_{i=1}^{h} \mathfrak{N}(\mathfrak{c}_i)^{-1/2} \ll \sum_{i=1}^{h} (i^{-1} \log^+ i)^{1/2} \ll (h \log^+ h)^{1/2}.$$

When $\Delta > 0$, each $\mathfrak{N}(\mathfrak{C})^{-1/2}$ is by (4.6) a sum of $2t$ terms $\mathfrak{N}(\mathfrak{c}_i)^{-1/2}$ with distinct integral ideals $\mathfrak{c}_i$ in $\mathfrak{C}$. Therefore the sum in (5.3) is a sum of $2th$ terms $\mathfrak{N}(\mathfrak{c}_i)^{-1/2}$. By the argument used above and since $t \ll R$ by (4.1), it is

$$\ll (2th \log^+(2th))^{1/2} \ll (Rh \log^+ Rh)^{1/2}.$$

6. Möbius inversion. In order not to have to interrupt our main argument below, we begin with the following definition. Given a nonzero ideal $\mathfrak{b}$, let $\langle \mathfrak{b} \rangle$ be its ideal class. Given an ideal class $\mathfrak{A}$, set

$$\mathfrak{L}_n(\mathfrak{A}) = \sum_{\mathfrak{b}} \mathfrak{N}(\mathfrak{A}\langle \mathfrak{b} \rangle)^{-1/2} \mathfrak{N}(\mathfrak{b})^{-n-1/2}, \tag{6.1}$$

where the sum is over integral ideals $\mathfrak{b}$ of the underlying quadratic field K. Since there are only h ideal classes, the term $\mathfrak{N}(\mathfrak{A}\langle \mathfrak{b} \rangle)^{-1/2}$ is bounded, and the sum will be convergent for $n > 0$, which we will suppose. Incidentally, it is easily seen, but will not be used here, that $\mathfrak{N}(\mathfrak{A}\langle \mathfrak{b} \rangle)^{-1/2} \le \mathfrak{N}(\mathfrak{A})^{-1/2} \mathfrak{N}(\mathfrak{b})^{1/2}$, so that when $n \ge 2$ we have

$$\mathfrak{L}_n(\mathfrak{A}) \le \mathfrak{N}(\mathfrak{A})^{-1/2} \sum_{\mathfrak{b}} \mathfrak{N}(\mathfrak{b})^{-n} \ll \mathfrak{N}(\mathfrak{A})^{-1/2}.$$

Lemmas 5, 10 may be combined to give

$$\begin{aligned} Z_2(\mathfrak{a}, \mathcal{S}, X) & \\ &= V_0(\mathcal{S}) R (X/|\Delta|^{1/2})^{n+1} + O(X^{n+(1/2)} |\Delta|^{-n/2} \mathfrak{N}(\mathfrak{A})^{-1/2}), \end{aligned} \tag{6.2}$$

where R is given by (1.4), and

$$V_0(\mathcal{S}) = \begin{cases} 2^{n+1} V(\mathcal{S}) & \text{when } \Delta < 0, \\ 2V(\mathcal{S}(e)) & \text{when } \Delta > 0. \end{cases} \tag{6.3}$$

Note that the hypotheses on $\mathcal{S}$ are not the same in the cases $\Delta < 0$ and $\Delta > 0$. Further recall that $Z_2(\mathfrak{a}, \mathcal{S}, X)$ is the number of nonzero $\boldsymbol{\alpha} = (\alpha_0, \ldots, \alpha_n) \in K^{n+1}$ such that

(i) $\alpha_i \in \mathfrak{a}$ $(i = 0, \ldots, n)$,
(ii) $\mathbb{Q}(P) = K$ where $P = (\alpha_0 : \ldots : \alpha_n)$,

(iii) $\widehat{\boldsymbol{\alpha}} \in (X\mathfrak{N}(\mathfrak{a}))^{1/2}\mathcal{S}$,

(iv) when $\Delta > 0$, additionally $\varepsilon^{-1} < \psi(\boldsymbol{\alpha}) \le \varepsilon$.

Let $Z_4(\mathfrak{a}, \mathcal{S}, X)$ be the number of nonzero $\boldsymbol{\alpha} \in K^{n+1}$ satisfying (i′), (ii), (iii), (iv), where (i′) is the condition

(i′) $\alpha_0, \ldots, \alpha_n$ generate the ideal $\mathfrak{a}$.

Lemma 12. *When* $\mathfrak{a}$ *lies in the ideal class* $\mathfrak{A}$,

$$Z_4(\mathfrak{a}, \mathcal{S}, X) = (V_0(\mathcal{S})R/\zeta_K(n+1))(X/|\Delta|^{1/2})^{n+1} + O(X^{n+(1/2)}|\Delta|^{-n/2}\mathfrak{L}_n(\mathfrak{A})).$$

P r o o f. When $\alpha_0, \ldots, \alpha_n$ satisfy (i), they generate an ideal $\mathfrak{ab}$ where $\mathfrak{b}$ is integral. Then (iii) may be written as $\widehat{\boldsymbol{\alpha}} \in (X/\mathfrak{N}(\mathfrak{b}))^{1/2}\mathfrak{N}(\mathfrak{ab})^{1/2}\mathcal{S}$. Therefore every $\boldsymbol{\alpha}$ counted by $Z_2(\mathfrak{a}, \mathcal{S}, X)$ is counted by $Z_4(\mathfrak{ab}, \mathcal{S}, X/\mathfrak{N}(\mathfrak{b}))$ for some integral $\mathfrak{b}$, and

$$Z_2(\mathfrak{a}, \mathcal{S}, X) = \sum_{\mathfrak{b}} Z_4(\mathfrak{ab}, \mathcal{S}, X/\mathfrak{N}(\mathfrak{b})).$$

Let μ be the Möbius function on nonzero integral ideals of K, so that $\mu(\mathfrak{ab}) = \mu(\mathfrak{a})\mu(\mathfrak{b})$ when $\mathfrak{a}$, $\mathfrak{b}$ are coprime, and $\mu(\mathfrak{p}) = -1$, $\mu(\mathfrak{p}^2) = \mu(\mathfrak{p}^3) = \ldots = 0$ when $\mathfrak{p}$ is a prime ideal. Möbius inversion gives

$$Z_4(\mathfrak{a}, \mathcal{S}, X) = \sum_{\mathfrak{b}} \mu(\mathfrak{b}) Z_2(\mathfrak{ab}, \mathcal{S}, X/\mathfrak{N}(\mathfrak{b})). \tag{6.4}$$

By (6.2),

$$Z_2(\mathfrak{ab}, \mathcal{S}, X/\mathfrak{N}(\mathfrak{b})) = V_0(\mathcal{S})R(X/\mathfrak{N}(\mathfrak{b})|\Delta|^{1/2})^{n+1} + O(X^{n+(1/2)}|\Delta|^{-n/2}\mathfrak{N}(\langle\mathfrak{ab}\rangle)^{-1/2}\mathfrak{N}(\mathfrak{b})^{-n-1/2}).$$

Since $\langle\mathfrak{ab}\rangle = \mathfrak{A}\langle\mathfrak{b}\rangle$ for $\mathfrak{a} \in \mathfrak{A}$, and since $\sum_{\mathfrak{b}} \mu(\mathfrak{b})\mathfrak{N}(\mathfrak{b})^{-n-1} = 1/\zeta_K(n+1)$, the lemma is a consequence of (6.4), (6.1).

7. Proof of Theorem 2. Let $\mathcal{S}$ be a closed set in $\mathbb{R}^{2n+2}$ as described in Sections 3, 4. Thus when $\Delta < 0$ we suppose that $\mathcal{S}$ is contained in the ball of radius 1 centered at the origin, and is of class m. We now make the further assumption that $\mathcal{S}$ contains the origin in its interior, and that $\boldsymbol{\phi}(\mathcal{S}) \subseteq \mathcal{S}$ for any linear transformation $\boldsymbol{\phi} : (\widehat{\alpha}_0, \ldots, \widehat{\alpha}_n) \mapsto (\phi(\widehat{\alpha}_0), \ldots, \phi(\widehat{\alpha}_n))$, where ϕ is a linear transformation of $\mathbb{R}^2$ which is an orthogonal map followed by a homothetic map $\widehat{\alpha} \mapsto t\widehat{\alpha}$ with $0 \le t \le 1$. When $\lambda \in K$ with $|\lambda| \le 1$, then $\widehat{\alpha} \mapsto \widehat{\lambda\alpha}$ where $\alpha \in K$ comes from a map ϕ as above, and therefore $\widehat{\boldsymbol{\alpha}} \in \mathcal{S}$ implies $(\widehat{\lambda\boldsymbol{\alpha}}) \in \mathcal{S}$. In general, when $\boldsymbol{\alpha} \in K^{n+1}$, then

$$\widehat{\boldsymbol{\alpha}} \in \mathcal{S} \quad \text{implies} \quad (\widehat{\lambda\boldsymbol{\alpha}}) \in |\lambda|\mathcal{S}. \tag{7.1}$$

When $\Delta > 0$, we suppose that $\mathcal{S}$ is contained in the set $|\boldsymbol{\alpha}|\,|\boldsymbol{\alpha}'| \le 2$, and it contains $\mathbf{0}$ in its interior. We will further suppose that when $(\boldsymbol{\alpha}, \boldsymbol{\alpha}') \in \mathcal{S}$, then so is $(t\boldsymbol{\alpha}, t'\boldsymbol{\alpha}')$ provided $t, t' \in \mathbb{R}$ have $|tt'| \le 1$. This amply yields the invariance property described in Section 4. Moreover, when $\boldsymbol{\alpha} \in K^{n+1}$ with $\widehat{\boldsymbol{\alpha}} \in \mathcal{S}$ and when $|\mathfrak{N}(\lambda)| = |\lambda\lambda'| \le 1$, then $(\widehat{\lambda\boldsymbol{\alpha}}) \in \mathcal{S}$. In general, $\boldsymbol{\alpha} \in K^{n+1}$ and

$$\widehat{\boldsymbol{\alpha}} \in \mathcal{S} \quad \text{implies} \quad (\widehat{\lambda\boldsymbol{\alpha}}) \in |\mathfrak{N}(\lambda)|^{1/2}\mathcal{S}. \tag{7.2}$$

As in Section 4, we will suppose that the intersection (denoted by $\mathcal{S}(x)$) of $\mathcal{S}$ and $x^{-1} < \psi(\boldsymbol{\alpha}) \le 1$ has closure of class m.

Given $\boldsymbol{\alpha} \in K^{n+1}$, let $H_\infty^{\mathcal{S}}(\boldsymbol{\alpha})$ be the least positive t with $\widehat{\boldsymbol{\alpha}} \in t\mathcal{S}$. From (7.1), (7.2) we conclude that

$$H_\infty^{\mathcal{S}}(\lambda\boldsymbol{\alpha}) = |\mathfrak{N}(\lambda)|^{1/2} H_\infty^{\mathcal{S}}(\boldsymbol{\alpha}). \tag{7.3}$$

Again, when $\boldsymbol{\alpha} \in K^{n+1}$, and $\boldsymbol{\alpha} \ne \mathbf{0}$, let $\mathfrak{a}$ be the ideal generated by $\alpha_0, \ldots, \alpha_n$, and set

$$H^{\mathcal{S}}(\boldsymbol{\alpha}) = (H_\infty^{\mathcal{S}}(\boldsymbol{\alpha}))^2/\mathfrak{N}(\mathfrak{a}).$$

By (7.3), and since $\lambda\boldsymbol{\alpha}$ induces the ideal $(\lambda)\mathfrak{a}$, it is clear that $H^{\mathcal{S}}(\lambda\boldsymbol{\alpha}) = H^{\mathcal{S}}(\boldsymbol{\alpha})$, so that we can define a height $H^{\mathcal{S}}(P)$ of points $P \in \mathbb{P}^n(K)$.

It is well known (see, e.g., [14, p. 11]) that when $\Delta < 0$ the field height is $H_K(\boldsymbol{\alpha}) = |\boldsymbol{\alpha}|^2/\mathfrak{N}(\mathfrak{a})$, so that $H_K(\boldsymbol{\alpha}) = H^{\mathcal{S}_0^-}(\boldsymbol{\alpha})$ with $\mathcal{S}_0^-$ the set in $\mathbb{R}^{2n+2}$ of points $(\xi_0, \eta_0, \ldots, \xi_n, \eta_n)$ with $\xi_i^2 + \eta_i^2 \le 1$ $(i = 0, \ldots, n)$. Here $V(\mathcal{S}_0^-) = \pi^{n+1}$, and

$$V_0(\mathcal{S}_0^-) = (2\pi)^{n+1} = \lambda^{n+1} = \nu\lambda^{n+1} \qquad (\Delta < 0) \tag{7.4}$$

by (6.3), (1.5), (1.7).

When $\Delta > 0$, the field height is $H_K(\boldsymbol{\alpha}) = |\boldsymbol{\alpha}|\,|\boldsymbol{\alpha}'|/\mathfrak{N}(\mathfrak{a}) = H^{\mathcal{S}_0^+}(\boldsymbol{\alpha})$, with $\mathcal{S}_0^+$ the set $|\boldsymbol{\alpha}|\,|\boldsymbol{\alpha}'| \le 1$. Here $\mathcal{S}_0^+(e)$ is further restricted by $e^{-1} < |\boldsymbol{\alpha}|/|\boldsymbol{\alpha}'| \le 1$, and a computation gives $V(\mathcal{S}_0^+(e)) = \frac{1}{2}(n+1) \cdot 4^{n+1}$. Therefore

$$V_0(\mathcal{S}_0^+) = (n+1) \cdot 4^{n+1} = \nu\lambda^{n+1} \qquad (\Delta > 0) \tag{7.5}$$

by (6.3), (1.5), (1.7).

Let $Z_5(K, \mathcal{S}, X)$ be the number of points $P \in \mathbb{P}^n(K)$ with $\mathbb{Q}(P) = K$ and $H^{\mathcal{S}}(P) \le X$.

Theorem 2a.

$$Z_5(K, \mathcal{S}, X) = \frac{hR}{w\zeta_K(n+1)} V_0(\mathcal{S})(X/|\Delta|^{1/2})^{n+1} + O(X^{n+(1/2)}|\Delta|^{-n/2}(hR\log^+ hR)^{1/2}).$$

Now $N'(K, n, X)$ is $Z_5(K, \mathcal{S}_0, X)$ with the set $\mathcal{S}_0 = \mathcal{S}_0^\pm$ described above. Theorem 2 follows on using (7.4), (7.5).

Proof of Theorem 2a. When $P = (\alpha_0 : \ldots : \alpha_n) \in \mathbb{P}^n(K)$, the ideal $\mathfrak{a}$ generated by $\alpha_0, \ldots, \alpha_n$ depends on P up to multiplication by a principal ideal, and therefore the ideal class $\mathfrak{A}$ of $\mathfrak{a}$ depends only on P. Let

$Z_6(\mathfrak{A}, \mathcal{S}, X)$ be the number of points $P \in \mathbb{P}^n(K)$ with $\mathbb{Q}(P) = K$ of height $H^{\mathcal{S}}(P) \le X$ belonging to the class $\mathfrak{A}$.

In the class $\mathfrak{A}$ pick an ideal $\mathfrak{a}$. Then when P belongs to the class $\mathfrak{A}$, we may write $P = (\alpha_0 : \ldots : \alpha_n)$ where $\alpha_0, \ldots, \alpha_n$ generate $\mathfrak{a}$. We have $H^{\mathcal{S}}(P) = (H^{\mathcal{S}}_\infty(\boldsymbol{\alpha}))^2/\mathfrak{N}(\mathfrak{a})$, so that $H^{\mathcal{S}}(P) \le X$ is the same as $H^{\mathcal{S}}_\infty(\boldsymbol{\alpha}) \le (X\mathfrak{N}(\mathfrak{a}))^{1/2}$, and this is the same as $\widehat{\boldsymbol{\alpha}} \in (X\mathfrak{N}(\mathfrak{a}))^{1/2}\mathcal{S}$. When $\Delta < 0$, then $\boldsymbol{\alpha}$ generating $\mathfrak{a}$ is determined by P up to multiplication by roots of 1, so that

$$Z_6(\mathfrak{A}, \mathcal{S}, X) = \frac{1}{w} Z_4(\mathfrak{a}, \mathcal{S}, X). \tag{7.6}$$

When $\Delta > 0$, $\boldsymbol{\alpha}$ may be chosen with $\varepsilon^{-1} < \psi(\boldsymbol{\alpha}) \le \varepsilon$, and is then unique up to a factor ± 1, so that (by the definition of $Z_4(\mathfrak{a}, \mathcal{S}, X)$ in this case) again (7.6) holds. Now $Z_4(\mathfrak{a}, \mathcal{S}, X)$ may be estimated by Lemma 12.

Theorem 2a follows by taking the sum over the ideal classes $\mathfrak{A}$. The main term is certainly correct. The error term will follow once we have shown that

$$\sum_{\mathfrak{A}} \mathfrak{L}_n(\mathfrak{A}) \ll (hR \log^+ hR)^{1/2};$$

here the sum is over all ideal classes $\mathfrak{A}$. But by the definition (6.1),

$$\sum_{\mathfrak{A}} \mathfrak{L}_n(\mathfrak{A}) = \Big(\sum_{\mathfrak{A}} \mathfrak{N}(\mathfrak{A})^{-1/2}\Big)\Big(\sum_{\mathfrak{b}} \mathfrak{N}(\mathfrak{b})^{-n-1/2}\Big).$$

The first factor is $\ll (hR \log^+ hR)^{1/2}$ by (5.3), and the second factor is

$$\zeta_K\left(n + \frac{1}{2}\right) \le \sum_{x=1}^{\infty} \tau(x) x^{-n-1/2} \ll 1,$$

where $\tau(x)$ is the number of divisors of x.

8. Proof of Theorem 3. Let $\mathcal{S}$ be a closed set in $\mathbb{R}^{2n+2}$ as specified in Section 7. More precisely, write $\mathcal{S} = \mathcal{S}^-$ if it is of the type specified for $\Delta < 0$, and $\mathcal{S} = \mathcal{S}^+$ if it is of the type specified for $\Delta > 0$. Let $H^{\mathcal{S}^+}(P)$ [or $H^{\mathcal{S}^-}(P)$] be the height of a point $P \in \mathbb{P}^n(A)$ where $\mathbb{Q}(P)$ is real quadratic (with discriminant $\Delta > 0$) [or imaginary quadratic (with $\Delta < 0$)]. With either the $+$ or $-$ sign, let $Z_7^{\pm}(\mathcal{S}^{\pm}, X)$ be the number of points $P \in \mathbb{P}^n(A)$ where $\mathbb{Q}(P)$ is quadratic with $\pm\Delta > 0$ and with $H^{\mathcal{S}^{\pm}}(P) \le X$. In what follows, for simplicity of notation, $\mathcal{S}$ will be a set of type $\mathcal{S}^+$ when dealing with Z_7^+, and of type $\mathcal{S}^-$ when dealing with Z_7^-.

THEOREM 3a. *When $n \ge 3$, then*

$$Z_7^{\pm}(\mathcal{S}, X) = c_{13}^{\pm}(\mathcal{S}) X^{n+1} + O(X^{n+(1/2)}) \tag{8.1}$$

with certain constants $c_{13}^+(\mathcal{S})$, $c_{13}^-(\mathcal{S})$ defined below. When $n = 2$, then

$$Z_7^{\pm}(\mathcal{S}, X) = c_{14}^{\pm}(\mathcal{S}) X^3 \log X + O(X^3 \sqrt{\log X}), \tag{8.2}$$

where

$$(8.3)\qquad c_{14}^{+}(\mathcal{S}) = V(\mathcal{S}(e))/(2\zeta(3)^2), \qquad c_{14}^{-}(\mathcal{S}) = 4V(\mathcal{S})/(\pi\zeta(3)^2).$$

Since $\mathcal{N}^{\pm}(2,n,X) = Z_7^{\pm}(\mathcal{S}_0^{\pm},X)$, and since by what we said in §7, $V(\mathcal{S}_0^{+}(e)) = 96$, $V(\mathcal{S}_0^{-}) = \pi^3$ for $n = 2$, we obtain the cases $n \ge 2$ of Theorem 3. The case $n = 1$ of that theorem will be dealt with in the next section.

P r o o f o f T h e o r e m 3a. It will be convenient to parametrize quadratic number fields by their discriminant Δ. Let $\mathcal{D}$ be the set of fundamental discriminants, i.e., the set of integers which arise as the discriminant of a quadratic number field. It is well known ([6, §29]) that $\mathcal{D} = \mathcal{D}_0 \cup \mathcal{D}_1$, where

$$\mathcal{D}_0 = \{\Delta = 4d \mid d \equiv 2 \text{ or } 3 \pmod 4,\ d \text{ square free}\},$$
$$\mathcal{D}_1 = \{\Delta \mid \Delta \equiv 1 \pmod 4,\ \Delta \text{ square free},\ \Delta \ne 1\}.$$

For $\Delta \in \mathcal{D}$ we will write $h = h(\Delta)$, $R = R(\Delta)$, $w = w(\Delta)$, etc., for the class number, regulator (as defined in (1.4)), number of roots of unity, etc., of the quadratic field with discriminant Δ. Also, with $Z_5(K,\mathcal{S},X)$ the quantity introduced in the last section, we will write $Z_5(\Delta,\mathcal{S},X) = Z_5(K,\mathcal{S},X)$ where K is the field with discriminant Δ. Now if $\mathcal{D}^{+}$, $\mathcal{D}^{-}$ consist respectively of positive and negative elements of $\mathcal{D}$, then

$$Z_7^{\pm}(\mathcal{S},X) = \sum_{\Delta\in\mathcal{D}^{\pm}} Z_5^{\pm}(\Delta,\mathcal{S},X).$$

Suppose initially that $n \ge 3$. Since, as is well known (see, e.g., [16]), $hR \ll |\Delta|^{1/2+\delta}$ for $\delta > 0$, the sum $\sum |\Delta|^{-n/2}(hR\log^{+} hR)^{1/2}$ over $\Delta \in \mathcal{D}$ is convergent. From Theorem 2a we may infer that (8.1) holds with

$$c_{13}^{\pm}(\mathcal{S}) = V_0(\mathcal{S}) \sum_{\Delta\in\mathcal{D}^{\pm}} \frac{h(\Delta)R(\Delta)}{w(\Delta)\zeta_{\Delta}(n+1)|\Delta|^{(n+1)/2}}.$$

Here we used the fact that the infinite sum in the definition of $c_{13}^{\pm}(\mathcal{S})$ is clearly convergent when $n \ge 3$.

This same sum is divergent when $n = 2$. When $n = 2$ we will use the fact that for a point $P \in \mathbb{P}^n(A)$ with $\mathbb{Q}(P)$ of degree d, the discriminant Δ of $\mathbb{Q}(P)$ has

$$(8.4)\qquad |\Delta| \le d^d H_K(P)^{2d-2}$$

(Silverman [18, Theorem 2]). In our case, $d = 2$, so that $|\Delta| \le 4H_K(P)^2$. The hypothesis that $\mathcal{S}$ is contained in the ball of radius 1 when $\Delta < 0$, and is contained in $|\boldsymbol{\alpha}|\,|\boldsymbol{\alpha}'| \le 2$ when $\Delta > 0$, implies that $H_K(P) \le c_{15}H^{\mathcal{S}}(P)$. Therefore $H^{\mathcal{S}}(P) \le X$ yields

$$|\Delta| \le c_{16}X^2.$$

Setting

(8.5) $$Y = c_{16} X^2,$$

and denoting the intersection of $\mathcal{D}$ or $\mathcal{D}^{\pm}$ with $|\Delta| \le Y$ by $\mathcal{D}(Y)$ or $\mathcal{D}^{\pm}(Y)$, we may infer from Theorem 2a that in the case $n = 2$ we have

(8.6) $$Z_7^{\pm}(\mathcal{S}, X) = A^{\pm} X^3 + O(BX^{5/2}),$$

where

$$A^{\pm} = V_0(\mathcal{S}) \sum_{\Delta \in \mathcal{D}^{\pm}(Y)} \frac{hR}{w(\Delta)\zeta_\Delta(3)|\Delta|^{3/2}},$$

$$B = \sum_{\Delta \in \mathcal{D}(Y)} |\Delta|^{-1}(hR \log^+ hR)^{1/2}.$$

We first turn to the evaluation of $A^{\pm}$. Let $\left(\frac{\Delta}{l}\right)$ be the Kronecker symbol, and

$$L(s, \Delta) = \sum_{l=1}^{\infty} \left(\frac{\Delta}{l}\right) l^{-s}$$

the L-function belonging to the quadratic field with discriminant Δ. Then

$$\zeta_\Delta(s) = \zeta(s) L(s, \Delta)$$

(Hecke [6, (137)]). Further

$$\frac{\lambda h R}{w|\Delta|^{1/2}} = L(1, \Delta)$$

by [6, (145)], our definition (1.5) of λ, and Hecke's definition of κ [6, p. 156]. Therefore

$$\frac{hR}{w\zeta_\Delta(3)|\Delta|^{3/2}} = \frac{L(1, \Delta)}{\lambda \zeta(3)|\Delta| L(3, \Delta)}.$$

In the appendix it will be shown that

(8.7) $$\sum_{\Delta \in \mathcal{D}^{\pm}(T)} L(1, \Delta)/L(3, \Delta) = (2\zeta(3))^{-1} T + O(T^{7/10+\delta}).$$

Partial summation gives

$$\sum_{\Delta \in \mathcal{D}^{\pm}(Y)} L(1, \Delta)/(L(3, \Delta)|\Delta|) = (2\zeta(3))^{-1} \log Y + O(1).$$

A combination of our equations yields

$$A^{\pm} = \frac{V_0(\mathcal{S})}{2\zeta(3)^2 \lambda}(\log Y + O(1)) = \frac{V_0(\mathcal{S})}{\zeta(3)^2 \lambda} \log X + O(1)$$

by (8.5), and since $V_0(\mathcal{S}) \ll 1$.

When dealing with A^+, we have $V_0(\mathcal{S}) = 2V(\mathcal{S}(e))$, $\lambda = 4$ by (6.3), (1.5), and when dealing with A^- we have $V_0(\mathcal{S}) = 8V(\mathcal{S})$, $\lambda = 2\pi$. Therefore

$$A^{\pm} = c_{14}^{\pm}(\mathcal{S}) \log X + O(1) \tag{8.8}$$

with $c_{14}^{\pm}(\mathcal{S})$ given by (8.3).

Let us turn to the quantity B. Since $hR \ll |\Delta|$ (in fact $\ll |\Delta|^{1/2+\delta}$),

$$B \ll (\log^+ Y)^{1/2} \sum_{\Delta \in \mathcal{D}(Y)} |\Delta|^{-3/8}((hR)^{1/2}|\Delta|^{-5/8}),$$

and by Cauchy's inequality this is

$$\ll (\log^+ Y)^{1/2}\Big(\sum_{|\Delta| \in \mathcal{D}(Y)} |\Delta|^{-3/4}\Big)^{1/2}\Big(\sum_{\Delta \in \mathcal{D}(Y)} hR|\Delta|^{-5/4}\Big)^{1/2}.$$

The first sum on the right hand side is $\ll Y^{1/4}$. On the other hand, for $T > 1$ we have

$$\sum_{\Delta \in \mathcal{D}(T)} hR \ll T^{3/2}$$

(see, e.g., Siegel [16], or the discussion in our appendix), and partial summation yields

$$\sum_{\Delta \in \mathcal{D}(Y)} hR/|\Delta|^{5/4} \ll Y^{1/4}.$$

We may conclude that

$$B \ll Y^{1/4}(\log^+ Y)^{1/2} \ll X^{1/2}(\log X)^{1/2}. \tag{8.9}$$

The estimate (8.2) now follows from (8.6), (8.8), (8.9).

9. The case $n = 1$ of Theorem 3. This case is easy and is independent of what has been done above. With the exception of $(0 : 1)$, every point of $\mathbb{P}^1$ is of the type $(1 : \alpha)$. When α is quadratic, it satisfies a unique equation $f(\alpha) = 0$, where

$$f(x) = ax^2 + bx + c$$

is a polynomial in $\mathbb{Z}[x]$ with $a > 0$, $\gcd(a, b, c) = 1$, which is irreducible over $\mathbb{Q}$. When $\mathfrak{a}$ is the fractional ideal generated by 1, α, then it follows from Gauss' Lemma that $\mathfrak{N}(\mathfrak{a}) = a^{-1}$, and therefore

$$H_K(1 : \alpha) = a \max(1, |\alpha|) \max(1, |\alpha'|),$$

where α' is the conjugate of α. The right hand side here is called the *Mahler measure* of α.

Suppose $\mathbb{Q}(\alpha)$ is imaginary quadratic. Then $c > 0$, $b^2 < 4ac$ and $|\alpha| = |\alpha'|$, so that $H_K(1 : \alpha) = \max(|a|, |c|)$. Therefore $\mathcal{N}^-(2, 1, X)$ is twice the number of irreducible polynomials $f(x)$ with

$$(9.1) \qquad 0 < a \le X, \quad 0 < c \le X, \quad |b| < 2\sqrt{ac},$$

and with $\gcd(a, b, c) = 1$. Since there are no reducible polynomials with negative discriminant, $\mathcal{N}^-(2, 1, X)$ *is twice the number of primitive integer points* (a, b, c) *in the region* $\mathcal{R}^-$ *given by* (9.1); here a point is *primitive* if its coordinates are coprime. The region $\mathcal{R}^-$ has volume $(16/9)X^3$, and it is contained in a ball of radius $\ll X$. Thus when $X \ge 1$, the number of integer points in this region is $(16/9)X^3 + O(X^2)$. This follows, e.g., from Davenport's inequality (2.4). By Möbius inversion, the number of primitive integer points in the region is $((16/9)\zeta(3))X^3 + O(X^2)$. We may conclude that

$$\mathcal{N}^-(2, 1, X) = ((32/9)\zeta(3))X^3 + O(X^2).$$

Suppose $\mathbb{Q}(\alpha)$ is real quadratic. Then $b^2 > 4ac$ and

$$\begin{aligned} H_K(1 : \alpha) &= \max(|a|, |c|, |a\alpha|, |a\alpha'|) \\ &= \max\left(|a|, |c|, \frac{1}{2}|b + \sqrt{b^2 - 4ac}|, \frac{1}{2}|b - \sqrt{b^2 - 4ac}|\right). \end{aligned}$$

Thus $H_K(\alpha) \le X$ means that $|a| \le X$, $|c| \le X$, and $|b| + \sqrt{b^2 - 4ac} \le 2X$. This last condition is the same as $b^2 - 4ac \le (2X - |b|)^2$, or $|b| \le X + (ac/X)$, so that

$$(9.2) \qquad 0 < a \le X, \quad |c| \le X, \quad b^2 > 4ac, \quad |b| \le X + (ac/X).$$

There are only few reducible polynomials with coefficients in this range: for if $f(x) = (ux + v)(u'x + v')$, then (as is well known—in fact it follows from (10.6) below)

$$\max(|u|, |v|) \max(|u'|, |v'|) \ll \max(|a|, |b|, |c|) < 2X.$$

Given nonnegative integers ν, ν' with $\nu + \nu' = [\log 2X]$, the number of integers u, v, u', v' with $\max(|u|, |v|) \ll e^{\nu}$, $\max(|u'|, |v'|) \ll e^{\nu'}$ is $\ll e^{2\nu + 2\nu'} \ll X^2$. Taking the sum over pairs ν, ν', we obtain $\ll X^2 \log X$ reducible polynomials. Therefore *up to a summand* $O(X^2 \log X)$, our $\mathcal{N}^+(2, 1, X)$ is twice the number of primitive integer points in the region $\mathcal{R}^+$ given by (9.2). We obtain

$$\mathcal{N}^+(2, 1, X) = 2V/\zeta(3) + O(X^2 \log X),$$

where V is the volume of $\mathcal{R}^+$. Write $\mathcal{R}^+ = \mathcal{R}_1^+ \cup \mathcal{R}_2^+$ with $\mathcal{R}_1^+, \mathcal{R}_2^+$ containing points with $c \le 0$ and $c > 0$, respectively. Setting $c_1 = -c$, we have

$$V(\mathcal{R}_1^+) = 2 \int_0^X \int_0^X (X - (ac_1/X))\, da\, dc_1 = (3/2)X^3,$$

$$V(\mathcal{R}_2^+) = 2 \int_0^X \int_0^X (X + (ac/X) - 2\sqrt{ac})\, da\, dc = (13/18)X^3.$$

Therefore $V = V(\mathcal{R}_1^+) + V(\mathcal{R}_2^+) = (20/9)X^3$. The case $n = 1$ of Theorem 3 follows.

10. Proof of Theorem 4. Given a nonzero quadratic form as in (1.9), with rational coefficients a_{ij}, let $H(f)$ be the height of its coefficient vector. Proportional forms have the same height. Let $Z_8(n, X)$ be the number of nonzero decomposable quadratic forms as above with height $H(f) \le X$, where proportional forms are counted as one. As was pointed out in the introduction, when f is decomposable, it determines a field $K(f)$. Let $Z_8^-(n, X)$, $Z_8^+(n, X)$, $Z_8^0(n, X)$ respectively count only those of the forms counted by $Z_8(n, X)$ where $K(f)$ is imaginary quadratic, real quadratic, or the rational field.

Theorem 4a.

$$Z_8^\pm(2, X) = c_{17}^\pm(2)X^3 \log X + O(X^3\sqrt{\log X}),$$

$$Z_8^\pm(n, X) = c_{17}^\pm(n)X^{n+1} + O(X^{n+(1/2)}) \qquad \textit{when } n \ge 3,$$

$$Z_8^0(n, X) = c_{17}^0(n)X^{n+1} \log X + O(X^{n+1}) \qquad \textit{when } n \ge 2.$$

This easily implies Theorem 4. For when f has coefficients $a_{ij} \in \mathbb{Z}$ with $|a_{ij}| \le X$, then uniquely $f = tf^*$ where t is natural and f^* has coprime coefficients $a_{ij}^* \in \mathbb{Z}$. Now

$$H(f^*) = \max_{i,j} |a_{ij}^*| = t^{-1} \max_{i,j} |a_{ij}| \le t^{-1}X,$$

so that (since Z_8 counts $\pm f^*$ as one, but $\mathcal{Z}$ counts $\pm f$ separately)

$$\mathcal{Z}^\pm(n, X) = 2 \sum_{t=1}^{\infty} Z_8^\pm(n, X/t). \tag{10.1}$$

When $t \le X$, we may apply Theorem 4a to $Z_8^\pm(n, X/t)$, and when $t > X$ we have $Z_8^\pm(n, X/t) = 0$. Thus, e.g., when $n = 2$, we have

$$\begin{aligned}\mathcal{Z}^\pm(2, X) &= 2c_{17}^\pm(2) \sum_{t=1}^{X} (X/t)^3 \log(X/t) + O\Big(\sum_{t=1}^{X} (X/t)^3 \sqrt{\log X}\Big) \\ &= 2\zeta(3)c_{17}^\pm(2)X^3 \log X + O(X^3\sqrt{\log X}).\end{aligned}$$

Therefore the first assertion of Theorem 4 holds with $c_8^{\pm}(2) = 2\zeta(3)c_{17}^{\pm}(2)$. The other cases of Theorem 4 follow similarly.

Proof of Theorem 4a. We begin with the quantities $Z_8^{\pm}(n, X)$. Let P, P' be the pair of points associated with the quadratic form f, as exhibited in the introduction, so that $\mathbb{Q}(P) = \mathbb{Q}(P') = K(f)$ is quadratic. We may represent P, P' as $(\alpha_0 : \ldots : \alpha_n)$, $(\alpha'_0 : \ldots : \alpha'_n)$, where $\alpha_i, \alpha'_i \in K(f)$ and α'_i is the conjugate of α_i $(0 \le i \le n)$. Then f is proportional to, and may be supposed to be equal to ll' with $l(\boldsymbol{x}) = \sum_{i=0}^n \alpha_i x_i$, $l'(\boldsymbol{x}) = \sum_{i=0}^n \alpha'_i x_i$. Let $\mathfrak{a}$ be the ideal generated in $K(f)$ by $\alpha_0, \ldots, \alpha_n$, and $\mathfrak{a}'$ be the ideal generated in $K(f)$ by $\alpha'_0, \ldots, \alpha'_n$. Further let $\mathfrak{u}$ be the ideal generated by the coefficients a_{ij} of f. By Gauss' Lemma, $\mathfrak{u} = \mathfrak{a}\mathfrak{a}'$, so that with $K = K(f)$, the respective norms have $\mathfrak{N}_{\mathbb{Q}}(\mathfrak{u})^2 = \mathfrak{N}_K(\mathfrak{u}) = \mathfrak{N}_K(\mathfrak{a})\mathfrak{N}_K(\mathfrak{a}') = \mathfrak{N}_K(\mathfrak{a})^2$. Therefore

$$H(f) = \mathfrak{N}_K(\mathfrak{a})^{-1} \max_{k,j} |a_{kj}|.$$

But

$$a_{kj} = \begin{cases} \alpha_k \alpha'_k & \text{when } k = j, \\ \alpha_k \alpha'_j + \alpha_j \alpha'_k & \text{when } k \ne j, \end{cases}$$

so that

$$H(f) = H^{\mathcal{S}}(P) \tag{10.2}$$

with a certain set $\mathcal{S} \subset \mathbb{R}^{2n+2}$. Namely, when we deal with Z_8^+, so that $K = K(f)$ is real, then $\mathcal{S} = \mathcal{S}_1^+$, say, is defined by

$$\begin{aligned} |\alpha_k \alpha'_k| &\le 1 \quad (0 \le k \le n), \\ |\alpha_k \alpha'_j + \alpha_j \alpha'_k| &\le 1 \quad (0 \le j < k \le n). \end{aligned} \tag{10.3}$$

Clearly when $(\boldsymbol{\alpha}, \boldsymbol{\alpha}') \in \mathcal{S}_1^+$ and $|tt'| \le 1$, then also $(t\boldsymbol{\alpha}, t'\boldsymbol{\alpha}') \in \mathcal{S}_1^+$. Furthermore, if k, j are chosen with $|\boldsymbol{\alpha}| = |\alpha_k|$, $|\boldsymbol{\alpha}'| = |\alpha'_j|$, then when $j \ne k$,

$$|\boldsymbol{\alpha}|\,|\boldsymbol{\alpha}'| = |\alpha_k|\,|\alpha'_j| \le 1 + |\alpha_j \alpha'_k| \le 1 + |\alpha_k|^{-1}|\alpha'_j|^{-1} = 1 + |\boldsymbol{\alpha}|^{-1}|\boldsymbol{\alpha}'|^{-1},$$

so that certainly $|\boldsymbol{\alpha}|\,|\boldsymbol{\alpha}'| < 2$. This is also true when $j = k$. If we deal with Z_8^-, so that $K = K(f)$ is imaginary quadratic, then α'_j is the complex conjugate of α_j, i.e., $\alpha'_j = \overline{\alpha}_j$, and (10.3) says that $|\alpha_k| \le 1$ $(0 \le k \le n)$ and $|2\,\mathrm{Re}(\alpha_k \overline{\alpha}_j)| \le 1$ $(0 \le j < k \le n)$. Writing $\alpha_k = \xi_k + i\eta_k$ with real ξ_k, η_k, we see that (10.2) holds with $\mathcal{S} = \mathcal{S}_1^-$ given by

$$\begin{aligned} \xi_k^2 + \eta_k^2 &\le 1 \quad (0 \le k \le n), \\ 2|\xi_k \xi_j + \eta_k \eta_j| &\le 1 \quad (0 \le j < k \le n). \end{aligned} \tag{10.4}$$

To each form f there belong the two points P, P'. Therefore

$$Z_8^{\pm}(n, X) = \tfrac{1}{2} Z_7^{\pm}(\mathcal{S}_1^{\pm}, X).$$

The first two assertions of Theorem 4a now follow from Theorem 3a. In fact, we have $c_{17}^{\pm}(n) = \frac{1}{2} c_{13}^{\pm}(\mathcal{S}_1^{\pm})$ when $n \ge 3$, $c_{17}^{\pm}(2) = \frac{1}{2} c_{14}^{\pm}(\mathcal{S}_1^{\pm})$ when $n = 2$.

We next turn to the quantity $Z_8^0(n,X)$. Our work here is independent of the rest of the paper. We may suppose that the coefficients a_{ij} of f are relatively prime integers. When f is reducible with $K(f)=\mathbb{Q}$, then $f=ll'$ with $l=\sum\alpha_i x_i$, $l'=\sum\alpha_i' x_i$, where $\boldsymbol{\alpha}=(\alpha_0,\ldots,\alpha_n)$, $\boldsymbol{\alpha}'=(\alpha_0',\ldots,\alpha_n')$ are *primitive* points, i.e., points with coordinates in $\mathbb{Z}$, and without common factor. Writing

$$G(\boldsymbol{\alpha},\boldsymbol{\alpha}')=\max(|\alpha_k\alpha_k'|\ (0\le k\le n)\text{ and }|\alpha_k\alpha_j'+\alpha_j\alpha_k'|\ (0\le j<k\le n)),$$

we have to deal with pairs of primitive points $\boldsymbol{\alpha}$, $\boldsymbol{\alpha}'$ with

$$G(\boldsymbol{\alpha},\boldsymbol{\alpha}')\le X. \tag{10.5}$$

We have seen above that $G(\boldsymbol{\alpha},\boldsymbol{\alpha}')\le 1$, which is the same as (10.3), implies $|\boldsymbol{\alpha}|\,|\boldsymbol{\alpha}'|<2$, so that in general

$$\tfrac{1}{2}|\boldsymbol{\alpha}|\,|\boldsymbol{\alpha}'|\le G(\boldsymbol{\alpha},\boldsymbol{\alpha}')\le 2|\boldsymbol{\alpha}|\,|\boldsymbol{\alpha}'|. \tag{10.6}$$

When $\boldsymbol{\alpha}=\boldsymbol{\alpha}'$ or $\boldsymbol{\alpha}=-\boldsymbol{\alpha}'$, we have $G(\boldsymbol{\alpha},\boldsymbol{\alpha}')\ge\frac{1}{2}|\boldsymbol{\alpha}|^2$, so that (10.5) gives $|\alpha_i|\ll X^{1/2}$. The number of such pairs is $\ll X^{(n+1)/2}$, which is negligible. (They correspond to quadratic forms f of rank 1.) When $\boldsymbol{\alpha}$, $\boldsymbol{\alpha}'$ are not related as above, we note that the pair $\boldsymbol{\alpha}$, $\boldsymbol{\alpha}'$ gives the same quadratic form as $\boldsymbol{\alpha}'$, $\boldsymbol{\alpha}$, and again we get the same quadratic form (up to a factor ±1) if $\boldsymbol{\alpha}$ or $\boldsymbol{\alpha}'$ is replaced by minus itself. Therefore

$$Z_8^0(n,X)=\tfrac{1}{8}Z_9(n,X)+O(X^{(n+1)/2}), \tag{10.7}$$

where $Z_9(n,X)$ is the number of ordered pairs of primitive points $\boldsymbol{\alpha}$, $\boldsymbol{\alpha}'$ with (10.5).

Now let $Z_{10}(n,X)$ be the number of (not necessarily primitive) ordered pairs of nonzero integer points $\boldsymbol{\alpha}$, $\boldsymbol{\alpha}'$ with (10.5).

LEMMA 13.

$$Z_{10}(n,X)=c_{18}(n)X^{n+1}\log X+O(X^{n+1}).$$

This lemma easily gives what we want: Indeed, each $\boldsymbol{\alpha}$, $\boldsymbol{\alpha}'$ may uniquely be written as $\boldsymbol{\alpha}=t\boldsymbol{\beta}$, $\boldsymbol{\alpha}'=t'\boldsymbol{\beta}'$ with t, t' natural numbers and with $\boldsymbol{\beta}$, $\boldsymbol{\beta}'$ primitive; and then $G(\boldsymbol{\beta},\boldsymbol{\beta}')=G(\boldsymbol{\alpha},\boldsymbol{\alpha}')/(tt')$. Therefore

$$Z_{10}(n,X)=\sum_{t=1}^{\infty}\sum_{t'=1}^{\infty}Z_9(n,X/(tt')).$$

Of course, the summands vanish when tt' is large, more precisely when $tt'>2X$, since $G(\boldsymbol{\beta},\boldsymbol{\beta}')<1/2$ yields $|\boldsymbol{\beta}|\,|\boldsymbol{\beta}'|<1$ by (10.6). Möbius inversion in both t, t' gives

$$Z_9(n,X)=\sum_{t}\sum_{t'}\mu(t)\mu(t')Z_{10}(n,X/(tt')), \tag{10.8}$$

where again we may restrict to summands with $tt' \le 2X$. It is an easy exercise to deduce from Lemma 13 that

$$Z_9(n,X) = (c_{18}(n)/\zeta(n+1)^2)X^{n+1}\log X + O(X^{n+1}),$$

which in view of (10.7) gives the last assertion of Theorem 4a with $c^0_{17}(n) = c_{18}(n)/(8\zeta(n+1)^2)$.

Incidentally, in order to deal with $\mathcal{Z}^0(n,X)$ in Theorem 4, we could have avoided the twofold inversion (10.8) (but not a simple inversion) by considering pairs $\boldsymbol{\alpha}, \boldsymbol{\alpha}'$ where just $\boldsymbol{\alpha}$ is required to be primitive.

Finally, we turn to the proof of Lemma 13. Nonzero integer points $\boldsymbol{\alpha}$ have $|\boldsymbol{\alpha}| \ge 1$, so that $Z_{10}(n,X)$ is the number of integer points $(\boldsymbol{\alpha}, \boldsymbol{\alpha}')$ in the set $\mathcal{T} \subset \mathbb{R}^{2n+2}$ given by

$$G(\boldsymbol{\alpha}, \boldsymbol{\alpha}') \le X \quad \text{and} \quad |\boldsymbol{\alpha}| \ge 1,\ |\boldsymbol{\alpha}'| \ge 1. \tag{10.9}$$

We will estimate $Z_{10}(n,X)$ using Davenport's inequality (2.4). We will show that

$$V(\mathcal{T}) = c_{18}(n)X^{n+1}\log X + O(X^{n+1}) \tag{10.10}$$

and

$$V(\mathcal{T}') \ll X^{n+1} \tag{10.11}$$

for the projections $\mathcal{T}'$ of $\mathcal{T}$ on the coordinate planes of dimensions $< 2n+2$; and this clearly will yield the lemma.

In view of (10.9) and (10.6), $\mathcal{T}$ is contained in a ball of radius $\ll X$, so that (10.11) is certainly true for the projection on a plane of dimension $\le n+1$. Without loss of generality it will therefore suffice to prove (10.11) when $\mathcal{T}'$ is the orthogonal projection of $\mathcal{T}$ on the coordinate plane $\Pi(l,m)$ consisting of points $(\alpha_0, \ldots, \alpha_l, 0, \ldots, 0, \alpha'_0, \ldots, \alpha'_m, 0, \ldots, 0)$ with $l \ge 0$, $m \ge 0$. In fact, we may suppose that

$$0 \le l \le m \le n. \tag{10.12}$$

Writing $\mathcal{T}'(l,m)$ for this projection, we will show that

$$V(\mathcal{T}'(l,m)) \begin{cases} = c_{19}(m)X^{m+1}\log X + O(X^{m+1}) & \text{when } l = m, \\ \ll X^{m+1} & \text{when } l < m. \end{cases} \tag{10.13}$$

This will give both (10.11) (when $l + m < 2n$), as well as (10.10) (when $l = m = n$).

Points $(\boldsymbol{\alpha}, \boldsymbol{\alpha}')$ in $\mathcal{T}'(l,m)$ where $|\boldsymbol{\alpha}| < 1$ or $|\boldsymbol{\alpha}'| < 1$ make up a set of volume $\ll X^{m+1}$, since $\mathcal{T}$ lies in a ball of radius $\ll X$. Such points may be neglected in the estimation of $V(\mathcal{T}'(l,m))$. Therefore $\mathcal{T}'(m,m)$ may be replaced by $\mathcal{T}''(m,m)$, consisting of $(\boldsymbol{\alpha}, \boldsymbol{\alpha}') \in \mathbb{R}^{m+1} \times \mathbb{R}^{m+1}$ with $G(\boldsymbol{\alpha}, \boldsymbol{\alpha}') \le X$ and $|\boldsymbol{\alpha}| \ge 1$, $|\boldsymbol{\alpha}'| \ge 1$. Points $(\boldsymbol{\alpha}, \boldsymbol{\alpha}') \in \mathcal{T}'(l,m)$ certainly have $\frac{1}{2}|\boldsymbol{\alpha}|\,|\boldsymbol{\alpha}'| \le X$, so that for $l < m$ we note that $\mathcal{T}'(l,m) \subseteq \mathcal{T}''(l,m)$, consisting of $(\boldsymbol{\alpha}, \boldsymbol{\alpha}') \in \mathbb{R}^{l+1} \times \mathbb{R}^{m+1}$ with $\frac{1}{2}|\boldsymbol{\alpha}|\,|\boldsymbol{\alpha}'| \le X$ and $|\boldsymbol{\alpha}| \ge 1$, $|\boldsymbol{\alpha}'| \ge 1$. Therefore it will suffice to prove (10.13) with $\mathcal{T}''(l,m)$ in place of $\mathcal{T}'(l,m)$. Here $\mathcal{T}''(l,m)$ consists of $(\boldsymbol{\alpha},\boldsymbol{\alpha}')$ with

$$F(\boldsymbol{\alpha},\boldsymbol{\alpha}') \le X, \qquad |\boldsymbol{\alpha}| \ge 1,\ |\boldsymbol{\alpha}'| \ge 1,$$

where

$$F(\boldsymbol{\alpha},\boldsymbol{\alpha}') = \begin{cases} G(\boldsymbol{\alpha},\boldsymbol{\alpha}') & \text{when } l = m, \\ \frac{1}{2}|\boldsymbol{\alpha}|\,|\boldsymbol{\alpha}'| & \text{when } l < m. \end{cases}$$

Write $\boldsymbol{\alpha} = r\boldsymbol{\beta}$, $\boldsymbol{\alpha}' = r'\boldsymbol{\beta}'$ where $r > 0$, $r' > 0$ and $|\boldsymbol{\beta}| = |\boldsymbol{\beta}'| = 1$, so that $1/2 \le F(\boldsymbol{\beta},\boldsymbol{\beta}') \le 2$. Let $d\boldsymbol{\beta}$ be the l-dimensional volume element on the cube surface $\mathcal{C}(l)$ consisting of $\boldsymbol{\beta} \in \mathbb{R}^{l+1}$ with $|\boldsymbol{\beta}| = 1$. (This cube has $2(l+1)$ sides of volume 2^l, so that $\int_{\mathcal{C}(l)} d\boldsymbol{\beta} = 2(l+1)\cdot 2^l$.) We have $d\boldsymbol{\alpha} = r^l dr d\boldsymbol{\beta}$. Similarly, $d\boldsymbol{\alpha}' = r'^m dr' d\boldsymbol{\beta}'$. In terms of the coordinates r, r', $\boldsymbol{\beta}$, $\boldsymbol{\beta}'$, the set $\mathcal{T}''(l,m)$ is given by $r \ge 1$, $r' \ge 1$ and $rr'F(\boldsymbol{\beta},\boldsymbol{\beta}') \le X$. Thus when $X \ge 1$,

$$V(\mathcal{T}''(l,m)) = \int\limits_{\mathcal{C}(l)} d\boldsymbol{\beta} \int\limits_{\mathcal{C}(m)} d\boldsymbol{\beta}' \int\limits_{1}^{X/F} r^l\,dr \int\limits_{1}^{X/(rF)} r'^m\,dr',$$

where $F = F(\boldsymbol{\beta},\boldsymbol{\beta}')$. The inner double integral is

$$\begin{cases} ((m+1)F^{m+1})^{-1}X^{m+1}\log X + O(X^{m+1}) & \text{when } l = m, \\ \ll X^{m+1} & \text{when } l < m. \end{cases}$$

Therefore (10.13) holds with

$$c_{19}(m) = (m+1)^{-1} \int\limits_{\mathcal{C}(m)} \int\limits_{\mathcal{C}(m)} F(\boldsymbol{\beta},\boldsymbol{\beta}')^{-m-1}\,d\boldsymbol{\beta}\,d\boldsymbol{\beta}'.$$

Appendix. Certain sums involving L-series. As in Section 8, let

$$L(s,\Delta) = \sum_{n=1}^{\infty} \left(\frac{\Delta}{n}\right) n^{-s}.$$

Here $\left(\frac{\Delta}{n}\right)$ is the Kronecker symbol, defined for $\Delta \equiv 0$ or $1 \pmod 4$. Let $\mathcal{D}$ be the set of fundamental discriminants, and $\mathcal{D}^+(X)$, $\mathcal{D}^-(X)$ respectively the set of numbers $\Delta \in \mathcal{D}$ with $0 < \Delta \le X$ or $0 < -\Delta \le X$. We will study sums of the type

$$S^{\pm}(s,a,X) = \sum_{\Delta \in \mathcal{D}^{\pm}(X)} L(s,\Delta)/L(a,\Delta).$$

Our goal in this appendix will be a proof of the following

Proposition. *Suppose $s = \sigma + it$, $a = \alpha + ib$ with $5/8 < \sigma < \alpha$ and $5/4 < \alpha$. Then for $\delta > 0$,*

$$S^{\pm}(s,a,X) = c_0(s,a)X + O(X^{\max(1/2+\delta,3/2-(4/5)\sigma+\delta})$$

with

$$c_0(s,a)=\frac{1}{2}\zeta(2s)\prod_p(1-p^{-2}-p^{-2s-1}+p^{-2s-2}-p^{-s-a}+p^{-s-a-1}).$$

Remarks. Here and below, the constants implicit in $O(\ldots)$ and in $\ll$ may depend on δ, σ and α only. The case $s=1$, $a=3$ yields (8.7), since $c_0(1,3)=1/(2\zeta(3))$. Presumably, our conditions on α and σ could be relaxed. Our method also shows that

$$S^{\pm}(s,X)=\sum_{\Delta\in\mathcal{D}^{\pm}(X)}L(s,\Delta)$$

has $S^{\pm}(s,X)\sim c_0(s)X$ with

$$c_0(s)=\frac{1}{2}\zeta(2s)\prod_p(1-p^{-2}-p^{-2s-1}+p^{-2s-2}),$$

and with an error term as in the proposition. Sums similar to $S^{\pm}(s,X)$ were studied by Goldfeld and Hoffstein [4]. (They take sums over $\Delta\in\mathcal{D}$ with $\Delta\equiv 1 \pmod 4$ and $0<\pm\Delta\le X$, and with $\Delta\equiv 0 \pmod 4$ and $0<\pm\Delta\le 4X$. They only require that $\sigma\ge 1/2$. There is a slight mistake in their constant.) Since, as already noted in Section 8, $\lambda hR/w=|\Delta|^{1/2}L(1,\Delta)$, the sums $S^{\pm}(1,X)$ are related to sums

$$\sum_{\Delta\in\mathcal{D}^{\pm}(X)}h(\Delta)R(\Delta).$$

Asymptotic formulas for such sums, but in the context of quadratic forms, and with Δ only restricted by $\Delta\equiv 0$ or $1 \pmod 4$, had been conjectured by Gauss, and first proved by Lipschitz [9] in the case of summation over $0<-\Delta\le X$, and by Siegel [15] over $0<\Delta\le X$.

Our method will follow Siegel's.

We begin with a series of lemmas.

LEMMA 14. *Let $\mathcal{E}$ consist of the integers which are congruent to* $1,5,9,13$, 8, *or* $12 \pmod{16}$. *Let $\mathcal{E}^{\pm}(Y)$ be the set of $E\in\mathcal{E}$ with $0<\pm E\le Y$. Given natural l, set*

$$A_l^{\pm}(Y)=\sum_{E\in\mathcal{E}^{\pm}(Y)}\left(\frac{E}{l}\right).$$

Then

(i) $A_l^{\pm}(Y)\ll\min(Y,l^{1/2}\log^+ l)$ *when l is not a square.*

(ii) *When $l=u^2$, then*

(A1) $$A_l^{\pm}(Y)=u^{-1}\psi(u)\phi(u)Y+O(u),$$

where ϕ is Euler's function and

$$\psi(u) = \begin{cases} 3/8 & \text{when } u \text{ is odd,} \\ 1/2 & \text{when } u \text{ is even.} \end{cases}$$

Proof. (i) When l is odd, then $\left(\frac{E}{l}\right)$ is a character of modulus l, and this character is nontrivial when l is not a square. When E runs through a finite set of consecutive integers, the corresponding sum $\sum \left(\frac{E}{l}\right)$ is $\ll l^{1/2}\log^+ l$ by the Pólya–Vinogradov inequality (see, e.g., [1, Theorem 13.15]). Since $(l,16)=1$, the same is true when E runs through a finite set of consecutive elements of an arithmetic progression with common difference 16. Since $\mathcal{E}$ consists of 6 such progressions, the assertion follows.

Now let l be even. Write $\mathcal{E} = \mathcal{E}_0 \cup \mathcal{E}_1$, where $\mathcal{E}_0$ consists of integers $\equiv 8$ or $12 \pmod{16}$, and $\mathcal{E}_1$ of integers $\equiv 1 \pmod 4$. For l even and $E \in \mathcal{E}_0$, we have $\left(\frac{E}{l}\right) = 0$. We therefore may restrict ourselves to $E \in \mathcal{E}_1$. Write $l = l_1 l_2$ where l_1 is a power of 2, and l_2 is odd. Following Siegel we observe that

$$\varrho_1(E) = \left(\frac{4l_1}{E}\right)\left(\frac{E}{l_2}\right) \quad \text{and} \quad \varrho_2(E) = \left(\frac{-4l_1}{E}\right)\left(\frac{E}{l_2}\right)$$

are nontrivial characters $\bmod 4l$, and that

$$\tfrac{1}{2}(\varrho_1(E) + \varrho_2(E)) = \begin{cases} \left(\frac{E}{l}\right) & \text{when } E \in \mathcal{E}_1, \\ 0 & \text{otherwise.} \end{cases}$$

A sum $\sum \varrho_i(E)$ $(i = 1,2)$, where E runs through a finite set of consecutive numbers, again is $\ll l^{1/2}\log^+ l$ by Pólya–Vinogradov. The assertion follows.

(ii) When $l = u^2$, then $A_l^{\pm}(Y)$ is the number of $E \in \mathcal{E}^{\pm}(Y)$ with $(E,u) = 1$. When u is odd, this is the number of integers E which lie in certain 6 residue classes $\pmod{16}$, which are coprime to u and lie in the interval $0 < \pm E \le Y$. The number of such integers E in an interval of length $16u$ is $6\phi(u)$, so that $A_l^{\pm}(Y) = (6\phi(u)/16u)Y + O(u)$, giving (A1). When u is even, then $A_l^{\pm}(Y)$ is the number of integers $E \equiv 1 \pmod 4$ with $(E,u) = 1$ lying in the interval $0 < \pm E \le Y$. The number of such integers in an interval of length $2u$ is $\phi(u)$, so that $A_l^{\pm}(Y) = (\phi(u)/2u)Y + O(u)$, again yielding (A1).

Lemma 15. *Put* $B_l^{\pm}(X) = \sum_{\Delta \in \mathcal{D}^{\pm}(X)} \left(\frac{\Delta}{l}\right)$.

(i) *When l is not a square*,

$$B_l^{\pm}(X) \ll l^{1/4}(\log^+ l)^{1/2} X^{1/2}.$$

(ii) *When* $l = u^2$,

$$B_l^{\pm}(X) = u^{-1}\psi(u)\phi(u)\Big(\sum_{\substack{q=1\\(2u,q)=1}}^{\infty} \mu(q)q^{-2}\Big)X + O(X^{1/2}u). \tag{A2}$$

Proof. As in §8, write $\mathcal{D} = \mathcal{D}_0 \cup \mathcal{D}_1$, where $\mathcal{D}_0$ consists of fundamental discriminants $\Delta \equiv 0 \pmod 4$ (i.e., $\Delta = 4E$ with $E \equiv 2$ or $3 \pmod 4$, E square free), and $\mathcal{D}_1$ consists of fundamental discriminants $\Delta \equiv 1 \pmod 4$ (i.e., $\Delta \equiv 1 \pmod 4$, Δ square free, $\Delta \neq 1$). Now

$$\sum_{\Delta\in\mathcal{D}_0^{\pm}(X)} \left(\frac{\Delta}{l}\right) = \sum_{\substack{0<\pm E\le X/4\\ E\equiv 2 \text{ or } 3 \,(\mathrm{mod}\, 4)\\ E \text{ square free}}} \left(\frac{4E}{l}\right) = \sum_{q=1}^{\sqrt{X}} \mu(q) \sum_{\substack{0<\pm E\le X/4\\ E\equiv 2 \text{ or } 3 \,(\mathrm{mod}\, 4)\\ q^2\mid E}} \left(\frac{4E}{l}\right).$$

The outer sum is understood to be over integers q in $1 \le q \le \sqrt{X}$. The summands have $E = q^2E'$ with q odd and $E' \equiv 2$ or $3 \pmod 4$. We clearly may restrict ourselves to summands with $(l, q) = 1$. We therefore obtain

$$\sum_{\substack{q=1\\ (2l,q)=1}}^{\sqrt{X}} \mu(q) \sum_{\substack{0<\pm E'\le X/(4q^2)\\ E'\equiv 2 \text{ or } 3 \,(\mathrm{mod}\, 4)}} \left(\frac{4E'}{l}\right),$$

so that

$$\sum_{\Delta\in\mathcal{D}_0^{\pm}(X)} \left(\frac{\Delta}{l}\right) = \sum_{\substack{q=1\\ (2l,q)=1}}^{\sqrt{X}} \mu(q) \sum_{\substack{0<\pm E\le X/q^2\\ E\in\mathcal{E}_0}} \left(\frac{E}{l}\right).$$

A similar computation shows that this relation remains true if $\mathcal{D}_0$, $\mathcal{E}_0$ are replaced by $\mathcal{D}_1$, $\mathcal{E}_1$. Taking the sum we get

$$B_l^{\pm}(X) = \sum_{\substack{q=1\\ (2l,q)=1}}^{\sqrt{X}} \mu(q) \sum_{E\in\mathcal{E}^{\pm}(X/q^2)} \left(\frac{E}{l}\right).$$

When l is not a square, the inner sum is $\ll \min(l^{1/2}\log^+ l, X/q^2)$ by Lemma 14, so that we get

$$\ll \sum_{q=1}^{\infty} \min(l^{1/2}\log^+ l, X/q^2) \ll X^{1/2}l^{1/4}(\log^+ l)^{1/2}.$$

When $l = u^2$, the inner sum is

$$u^{-1}\psi(u)\phi(u)(X/q^2) + O(u)$$

by the same lemma. Thus

$$B_l^{\pm}(X) = u^{-1}\psi(u)\phi(u)\Big(\sum_{\substack{q=1\\ (2u,q)=1}}^{\sqrt{X}} \mu(q)q^{-2}\Big)X + O(X^{1/2}u),$$

from which we easily get (A2).

We now introduce a parameter $Z > 1$, to be specified later.

LEMMA 16. (i) *When* $\sigma > 0$,

$$L(s,\varDelta) = L_1(s,\varDelta,Z) + O(Z^{-\sigma}|\varDelta|^{1/2}\log^+|\varDelta|)$$

where

$$L_1(s,\varDelta,Z) = \sum_{n=1}^{Z}\left(\frac{\varDelta}{n}\right)n^{-s}.$$

(ii) *When* $a = \alpha + ib$, *with* $\alpha > 1$, *then* $|L(a,\varDelta)| \gg 1$.

Proof. (i) We may suppose that Z is an integer.

$$L(s,\varDelta) - L_1(s,\varDelta,Z) = \sum_{n>Z}\left(\frac{\varDelta}{n}\right)n^{-s} = \sum_{n>Z}(s_n - s_{n-1})n^{-s}$$

with

$$s_n := \sum_{j=1}^{n}\left(\frac{\varDelta}{j}\right) \ll |\varDelta|^{1/2}\log^+|\varDelta|$$

by Pólya–Vinogradov. We get

$$\begin{aligned} L(s,\varDelta) - L_1(s,\varDelta,Z) &= \sum_{n>Z} s_n(n^{-s} - (n+1)^{-s}) - s_Z(Z+1)^{-s} \\ &\ll |\varDelta|^{1/2}(\log^+|\varDelta|)\Big(\Big(\sum_{n>Z} n^{-\sigma-1}\Big) + Z^{-\sigma}\Big) \\ &\ll Z^{-\sigma}|\varDelta|^{1/2}\log^+|\varDelta|. \end{aligned}$$

(ii) follows from the product formula

$$|L(a,\varDelta)| = \prod_p \left|1 - \left(\frac{\varDelta}{p}\right)p^{-a}\right|^{-1} \geq \prod_p (1 + p^{-\alpha})^{-1} \gg 1.$$

We now turn to the proof of the proposition. By Lemma 16,

$$S^{\pm}(s,a,X) = \sum_{\varDelta\in\mathcal{D}^{\pm}(X)} \frac{L(s,\varDelta,Z)}{L(a,\varDelta)} + O\Big(Z^{-\sigma}\sum_{\varDelta=-X}^{X}|\varDelta|^{1/2}\log^+\varDelta\Big),$$

so that

(A3) $$S^{\pm}(s,a,X) = S_1^{\pm}(s,a,X,Z) + O(Z^{-\sigma}X^{3/2}\log X)$$

where (in view of $L(a,\varDelta)^{-1} = \sum_m \left(\frac{\varDelta}{m}\right)\mu(m)m^{-a}$),

(A4) $$S_1^{\pm}(s,a,X,Z) = \sum_{\varDelta\in\mathcal{D}^{\pm}(X)}\Big(\sum_{n=1}^{Z}\left(\frac{\varDelta}{n}\right)n^{-s}\Big)\Big(\sum_{m=1}^{\infty}\left(\frac{\varDelta}{m}\right)\mu(m)m^{-a}\Big)$$

$$= \sum_{m=1}^{\infty} \mu(m) m^{-a} \sum_{n=1}^{Z} n^{-s} \sum_{\Delta \in \mathcal{D}^{\pm}(X)} \left(\frac{\Delta}{mn}\right).$$

When mn is not a square, the inner sum is $\ll X^{1/2}(mn)^{1/4}(\log^+ mn)^{1/2}$ by Lemma 15. Therefore the terms with mn not a square contribute

$$\ll X^{1/2}\Big(\sum_{m=1}^{\infty} m^{1/4-\alpha}(\log^+ m)^{1/2}\Big)\Big(\sum_{n=1}^{Z} n^{1/4-\sigma}(\log^+ n)^{1/2}\Big),$$

and since $\alpha > 5/4$, this is

$$\ll X^{1/2} \max(1, Z^{5/4-\sigma})(\log^+ Z)^{3/2}.$$

Thus

$$\text{(A5)} \qquad S_1^{\pm}(s,a,X,Z) = S_2^{\pm}(s,a,X,Z) + O(X^{1/2}\max(1, Z^{5/4-\sigma})(\log^+ Z)^{3/2}),$$

where $S_2^{\pm}(s,a,X,Z)$ is the sum of the terms where mn is a square.

When $mn = u^2$, the inner sum on the right hand side of (A4) is again estimated by Lemma 15. We have

$$u^{-1}m^{-a}n^{-s} = u^{-2s-1}m^{s-a}, \qquad um^{-a}n^{-s} = u^{-2s+1}m^{s-a},$$

so that

$$\text{(A6)} \qquad S_2^{\pm}(s,a,X,Z) = XS_3(s,a,Z) + O(X^{1/2}S_3^*(s,a,Z)),$$

where

$$S_3(s,a,Z) = \sum_{m=1}^{\infty} \mu(m) m^{s-a} \sum_{\substack{u=1 \\ m\mid u^2}}^{\sqrt{mZ}} \psi(u)\phi(u)u^{-2s-1} \sum_{\substack{q=1 \\ (2u,q)=1}}^{\infty} \mu(q)q^{-2},$$

$$S_3^*(s,a,Z) = \sum_{m=1}^{\infty} m^{\sigma-\alpha} \sum_{\substack{u=1 \\ m\mid u^2}}^{\sqrt{mZ}} u^{-2\sigma+1} \ll \sum_{u=1}^{\infty} u^{1-2\sigma} \sum_{\substack{m\mid u^2 \\ m \ge u^2/Z}} m^{\sigma-\alpha}.$$

The number of divisors of u^2 is $\ll u^{\delta}$ for $\delta > 0$, so that the inner sum here is $\ll u^{\delta}\min(1, (Z/u^2)^{\alpha-\sigma})$, since $\alpha \ge \sigma$. Recalling that $\alpha > 1$, and choosing δ sufficiently small, we get

$$\text{(A7)} \qquad S_3^*(s,a,Z) \ll \sum_{u \le \sqrt{Z}} u^{1-2\sigma+\delta} + Z^{\alpha-\sigma} \sum_{u > \sqrt{Z}} u^{1-2\alpha+\delta} \ll \max(1, Z^{1-\sigma+\delta}).$$

It remains for us to deal with $S_3(s,a,Z)$. Since

$$\sum_{u>\sqrt{mZ}} \psi(u)\phi(u)u^{-2s-1} \ll \sum_{u>\sqrt{mZ}} u^{-2\sigma} \ll (mZ)^{1/2-\sigma},$$

and since $\sum_m m^{1/2-\alpha} \ll 1$, we have

$$S_3(s,a,Z) = c_0(s,a) + O(Z^{1/2-\sigma}) \tag{A8}$$

with

$$c_0(s,a) = \sum_{u=1}^{\infty} \psi(u)\phi(u)u^{-2s-1} \sum_{\substack{q=1\\(2u,q)=1}}^{\infty} \mu(q)q^{-2} \sum_{m|u} \mu(m)m^{s-a}.$$

Combining (A3), (A5), (A6), (A7), (A8) we obtain

$$S^{\pm}(s,a,X) = c_0(s,a)X + O(Z^{-\sigma}X^{3/2+\delta} + X^{1/2}Z^{\delta}\max(1, Z^{5/4-\sigma}) + XZ^{1/2-\sigma}).$$

We now choose $Z = X^{4/5}$ to obtain the estimate of the proposition.

To evaluate $c_0(s,a)$ we note that

$$\sum_{\substack{q=1\\(2u,q)=1}}^{\infty} \mu(q)q^{-2} = \zeta(2)^{-1}\prod_{p|2u}(1-p^{-2})^{-1} = \zeta(2)^{-1}\varrho(u)\prod_{p|u}(1-p^{-2})^{-1},$$

where $\varrho(u) = 1$ when u is even, $\varrho(u) = 4/3$ when u is odd. Note that $\psi(u)\varrho(u) = 1/2$ always. Therefore

$$c_0(s,a) = (2\zeta(2))^{-1}\sum_{u=1}^{\infty}\phi(u)u^{-2s-1}\Big(\prod_{p|u}(1-p^{-2})^{-1}(1-p^{s-a})\Big).$$

The function in u behind the $\sum$ symbol is multiplicative, so that

$$\begin{aligned}
c_0(s,a) &= (2\zeta(2))^{-1}\prod_p \Big(1 + (1-p^{-2})^{-1}(1-p^{s-a})\Big(\sum_{\nu=1}^{\infty}\phi(p^{\nu})/p^{\nu(2s+1)}\Big)\Big)\\
&= (2\zeta(2))^{-1}\\
&\quad \times \prod_p (1 + (1-p^{-2})^{-1}(1-p^{-(a-s)})(1-p^{-2s})^{-1}(p-1)p^{-2s-1})\\
&= \frac{1}{2}\zeta(2s)\prod_p((1-p^{-2})(1-p^{-2s}) + (1-p^{-(a-s)})(p-1)p^{-2s-1})\\
&= \frac{1}{2}\zeta(2s)\prod_p(1 - p^{-2} - p^{-2s-1} + p^{-2s-2} - p^{-a-s} + p^{-a-s-1}).
\end{aligned}$$

References

[1] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer, New York, 1976.

[2] J. W. S. Cassels, *An Introduction to the Geometry of Numbers*, Grundlehren Math. Wiss. 99, Springer, 1959.

[3] H. Davenport, *On a principle of Lipschitz*, J. London Math. Soc. 26 (1951), 179–183.

[4] D. Goldfeld and J. Hoffstein, *Eisenstein series of* $\frac{1}{2}$*-integral weight and the mean value of real Dirichlet L-series*, Invent. Math. 80 (1985), 185–208.

[5] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 3rd ed., Clarendon Press, Oxford, 1954.

[6] E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, Chelsea, 1948.

[7] Y. R. Katznelson, *Asymptotics for singular integral matrices in convex domains and applications*, Ph.D. Dissertation, Stanford Univ., 1991.

[8] S. Lang, *Fundamentals of Diophantine Geometry*, Springer, 1983.

[9] R. Lipschitz, Sitzungsber. Akad. Berlin, 1865, 174–185.

[10] D. G. Northcott, *An inequality in the theory of arithmetic on algebraic varieties*, Proc. Cambridge Philos. Soc. 45 (1949), 502–509 and 510–518.

[11] S. H. Schanuel, *Heights in number fields*, Bull. Soc. Math. France 107 (1979), 433–449.

[12] W. M. Schmidt, *Diophantine Approximations and Diophantine Equations*, Lecture Notes in Math. 1467, Springer, 1991.

[13] —, *Northcott's theorem on heights, I. A general estimate*, Monatsh. Math. 115 (1993), 169–181.

[14] J.-P. Serre, *Lectures on the Mordell–Weil Theorem*, Vieweg, Braunschweig, 1988.

[15] C. L. Siegel, *The average measure of quadratic forms with given determinant and signature*, Ann. of Math. 45 (1944), 667–685.

[16] —, *Abschätzung von Einheiten*, Nachr. Akad. Wiss. Göttingen, Math.-Phys. Kl. 1969, 71–86.

[17] —, *Lectures on the Geometry of Numbers*, rewritten by K. Chandrasekharan, Springer, 1988.

[18] J. Silverman, *Lower bounds for height functions*, Duke Math. J. 51 (1984), 395–403.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF COLORADO
BOULDER, COLORADO 80309-0395
U.S.A.

Received on 4.8.1992 (2290)