Y. Kitaoka
Nagoya Math. J.
Vol. 115 (1989), 23–41

SOME REMARKS ON REPRESENTATIONS OF POSITIVE DEFINITE QUADRATIC FORMS

YOSHIYUKI KITAOKA

Let S, T be positive definite integral symmetric matrices of degree m, n respectively and let us consider the quadratic diophantine equation $S[X] = T$. We know already [1] that the following assertion $(A)_{m,n}$ is true for $m \geq 2n + 3$.

$(A)_{m,n}$: There exists a constant $c(S)$ such that $S[X] = T$ has an integral solution $X \in M_{m,n}(Z)$ if $S[X] = T$ has an integral solution $X \in M_{m,n}(Z_p)$ for every prime p and $\min T > c(S)$.

In the above, $\min T$ denotes the minimum of $T[x]$ for all non-zero integral vectors x. The basic question is whether the number $2n + 3$ is best possible or not. As facts which suggest that $2n + 3$ is best, we can enumerate the following (i), (ii), (iii):

(i) When $n = 1$, it is the case.

(ii) From the quantitative viewpoint, the Siegel's weighted average of the numbers of solutions of $S_i[X] = T$ where S_i runs over a complete set of representatives of the classes in the genus of S, is expected to be not few if $(A)_{m,n}$ is true. By a Siegel's formula [9], the weighted average is $|T|^{(m-n-1)/2}$ times the infinite product of local densities $\alpha_p(s, T)$ up to the elementary constant depending only on S and n, and it is known [2] that there is a positive constant $c_1(s)$ such that the infinite product of local densities is larger than $c_1(S)$ as far as T is represented by S over Z_p for every prime p if and only if $m \geq 2n + 3$.

(iii) The condition $m \geq 2n + 3$ appears often naturally at an analytic approach.

Next, let us look at the problem from another viewpoint which leads us to the suggestion incompatible with the above observation for $n > 1$. It is known [2] that $(A)_{m,n}$ does not hold for $m = n + 3$. It is the best for all n till now, as far as the author knows. When $m = n + 3$, we

Received June 9, 1988.

https://doi.org/10.1017/S0027763000001501 Published online by Cambridge University Press

constructed counterexamples by the following idea. Suppose $S[X] = T$ for $X \in M_{m,n}(Z)$; writing $X = YZ$ with a primitive matrix $Y \in M_{m,n}(Z)$ and $Z \in M_{n,n}(Z)$, $\bar{T} := T[Z^{-1}] = S[Y]$ is (primitively represented globally by S and hence) primitively represented by S over Z_p, and it yields that min $\bar{T}$ is less than min S. This is a contradiction.

Now the following problem emerges along this line: Let S, T m, n be those as above, $S[X] = T$ is soluble over Z_p for every prime p, and min T is large. Then for every matrix $\bar{T}$ which satisfies

(i) $S[X] = \bar{T}$ has a primitive solution over Z_p for every prime p, and

(ii) $\bar{T}[X] = T$ is soluble for $X \in M_{n,n}(Z)$,

is min $\bar{T}$ small?

We have obtained counterexamples for $m = n + 3$ by showing the affirmative of this question. If it is affirmative for $m = 2n + 2$, then, reforming S, we must construct a counterexample for $(A)_{2n+2,n}$. When $m = 2n + 2$ and $n = 1$, it is affirmative and we have a counterexample for $(A)_{4,1}$. However it turns out to be negative for $m = 2n + 2$, $n \geq 2$, which is an aim of this paper, that is the following assertion $(R)_{m,n}$ is true for $m = 2n + 2$, $n \geq 2$ (Theorem in **1** in the text):

$(R)_{m,n}$: Let S, T m, n be those as above and suppose that $S[X] = T$ is soluble over Z_p for every prime p. Then there exists a positive integral matrix $\bar{T}$ of degree n satisfying

(i) $S[X] = \bar{T}$ has a primitive solution X over Z_p for every prime p,

(ii) $\bar{T}[X] = T$ is soluble for $X \in M_{n,n}(Z)$, and

(iii) if min T is large, then min $\bar{T}$ is also large.

Moreover in connection with primitiveness in (i), let us consider the following assertions:

$(AP)_{m,n}$: There exists a constant $c'(S)$ such that $S[X] = T$ has a primitive integral solution $X \in M_{m,n}(Z)$ if $S[X] = T$ has a primitive integral solution $X \in M_{m,n}(Z_p)$ for every prime p and min $T > c'(S)$.

$(APW)_{m,n}$: The weaker assertion than $(AP)_{m,n}$ which does not require the primitiveness of global solution.

Since $(A)_{2n+3,n}$ is true and $(APW)_{m,n}$ has a stronger assumption than $(A)_{m,n}$, one may expect the validity of $(APW)_{2n+2,n}$ or strongly $(AP)_{2n+2,n}$, taking account of the validity of $(AP)_{4,1}$ and hence $(APW)_{4,1}$. The weak assertion $(APW)_{2n+2,n}$ implies the assertion $(A)_{2n+2,n}$ by virtue of the validity of $(R)_{2n+2,n}$ for $n \geq 2$. If, hence $(A)_{2n+2,n}$ is false for $n \geq 2$, then

$(AP)_{2n+2,n}$ and $(APW)_{2n+2,n}$ are also false. Here we note again that $(R)_{4,1}$ is false and it yields immediately the falsehood of $(A)_{4,1}$ but $(AP)_{4,1}$ (and hence $(APW)_{4,1}$) is true. Results here and [3], [5], [6] may suggest the validity of $(A)_{2n+2,n}$ for $n \geq 2$. This dennies the suggestion at the beginning that $2n+3$ is best possible for $n \geq 2$. Which is plausible? In **2** in the text, we show that $(R)_{m,n}$ ($m \geq n+3$ and $n \geq 3$) is valid for scalings of a fixed T_0 with small limitation. It shows that it is hard to construct counterexamples for $(A)_{m,n}$ for $m \geq n+3$, $n \geq 3$ by a special sequence of T which are scalings of some fixed T_0.

Let us discuss the case of $m = 2n+2 \geq 6$ from the analytic viewpoint in passing. We put a fundamental assumption that for every Siegel modular form $f(Z) = \sum a(T) \exp(2\pi i \operatorname{tr} TZ)$ of degree n, weight $n+1$ and some level, whose constant term vanishes at each cusp, the estimate $a(T) = O((\min T)^{-\varepsilon} |T|^{(n+1)/2})$ holds for some positive ε if $\min T$ is larger than some constant independent of $f(Z)$. To verify the assertion $(A)_{2n+2,n}$ it is sufficient to do the assertion $(APW)_{2n+2,n}$ as above. Suppose that $S[X] = T$ has a primitive solution $X = X_p \in M_{m,n}(Z_p)$ for every prime p. Let $r_{\mathrm{pr}}(T, S)$ be the number of integral primitive solutions of $S[X] = T$. As in § 1.7 in [3] we have

$$r_{\mathrm{pr}}(T, S) = SW_p(T) + O((\min T)^{-\varepsilon_2} |T|^{(n+1)/2})$$

where $SW_p(T)$ is a quantity defined there so that

$$SW_p(T) \gg n(T)^{-\varepsilon_1} |T|^{(n+1)/2} > (\min T)^{-\varepsilon_1} |T|^{(n+1)/2},$$

and $\varepsilon_1, \varepsilon_2$ are any positive small number, and hence it gives an asymptotic formula for $r_{\mathrm{pr}}(T, S)$ when $\min T$ tends to the infinity and therefore $r_{\mathrm{pr}}(T, S) > 0$ when $\min T$ is sufficiently large, and thus the above assumption on estimates of $a(T)$ yields an asymptotic formula for $r_{\mathrm{pr}}(T, S)$ and the truth of the assertion $(A)_{2n+2,n}$. Let us refer to an asymptotic formula for the number of solutions $r(T, S)$ of $S[X] = T$. Denote by P a set of primes p such that the Witt index of S over $\boldsymbol{Q}_p$ is equal to $n-1$. The assumption on $a(T)$ yields an asymptotic formula for $r(T, S)$ if P is empty. Otherwise it depends on estimates of local densities from below for every prime $p \in P$ and the explicit value of ε whether it gives an asymptotic formula or not. The existence of an asymptotic formula may be harmonious.

We denote by $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{Z}_p$ and $\boldsymbol{Q}_p$ the ring of rational integers, the field of rational numbers and their p-adic completions respectively. Terminology and notations on quadratic forms are generally those from [6] and they are also used for symmetric matrices corresponding to quadratic forms. For example, for a quadratic lattice M over $\boldsymbol{Z}$, nM is the norm of M, i.e., $nM = \boldsymbol{Z}\{Q(x) \mid x \in M\}$, and for a basis $\{v_i\}$ of M we write $M = \langle (B(v_i, v_j)) \rangle$. By a positive lattice we mean a lattice on a positive definite quadratic space over $\boldsymbol{Q}$. For a positive lattice M, $\min M$ denotes the minimum of $\{Q(x) \mid x \in M,\ x \neq 0\}$, where $Q(x) = B(x, x)$ is the quadratic form of M.

§1.

In this section we prove the following

THEOREM. *Let m, n be integers such that $m = 2n + 2$ and $n \geq 2$ and let M be a positive lattice of $\operatorname{rank} M = m$ with $nM \subset 2\boldsymbol{Z}$. Let N be a positive lattice of $\operatorname{rank} N = n$ such that $\boldsymbol{Z}_pN$ is represented by $\boldsymbol{Z}_pM$ for each prime p. Put $nN = 2q\boldsymbol{Z}$ for a natural number q and decompose q as $q = q_0q_1$ so that, for a prime divisor p of q, p divides q_0 if and only if the Witt index of $\boldsymbol{Q}_pM$ is equal to $n - 1$. Then there exists a positive lattice $\bar{N}$ on $\boldsymbol{Q}N$ such that $\bar{N} \supset N$, $\min \bar{N} > c(M)\sqrt{q}_0^{-1} \min N$ and $\boldsymbol{Z}_p\bar{N}$ is primitively represented by $\boldsymbol{Z}_pM$ for each prime p where $c(M)$ is a positive constant dependent only on M.*

COROLLARY. *If $m = 2n + 2 \geq 6$, then the assertion $(APW)_{2n+2,n}$ yields $(A)_{2n+2,n}$.*

Before the proof of Theorem, we note that if we put $N = \langle qT \rangle$ where T is an integral positive matrix, then $\min N = q(\min T)$ and hence $\min \bar{N} > c(M)\sqrt{q_0}q_1 \min T$. Thus $\min \bar{N}$ is large if $\min N$ is large.

LEMMA 1. *Let a, u be real numbers such that $a > 1$ and $\sqrt{a}/4 < u < \sqrt{a}$. Put $f(x, y) = (ax - uy)^2 + y^2$. Then the minimum of $\{f(x, y) \mid x, y \in \boldsymbol{Z},\ (x, y) \neq (0, 0)\}$ is larger than $a/16$.*

Proof. $f(0, 1) = u^2 + 1 > u^2 > a/16$ and $f(1, 0) = a^2 > a/16$ are clear. Suppose $x, y \in \boldsymbol{Z}$ and $xy \neq 0$. If $|y| > \sqrt{a}/4$, then $f(x, y) \geq y^2 > a/16$. Assume $|y| \leq \sqrt{a}/4$. Since it implies $|uy| < a/4$, the minimum of $|ax - uy|$ $(x \in \boldsymbol{Z})$ is equal to $|uy|$. Hence $f(x, y) > (ax - uy)^2 \geq (uy)^2 \geq u^2 > a/16$ holds, which completes the proof of Lemma 1.

LEMMA 2. *Let p be a prime and $n \geq 2$. Let $T = p^{2b+c}T_0$ $(0 < b \in Z$, $c = 0, 1)$ be an integral positive definite matrix of degree n and suppose $p^b \geq 36$, $nT_0 \subset 2Z$ and $(nT_0)Z_p = 2Z_p$. Then there exists a positive constant $C(n, p)$ dependent on n and p for which there exists H in $M_n(Z)$ satisfying that $\det H$ is a power of p, $\min T[H^{-1}] > C(n, p)p^{b+c} \min T_0$, $T[H^{-1}] \not\equiv 0 \bmod 8p^{1+c}$ and $n(T[H^{-1}]) \subset 2Z$.*

Proof. Put $G = SL(n, Z)$, $G' = \{g \in G \mid g \equiv 1_n \bmod 8pZ_p\}$, take and fix representatives $\{U_i\}$ of G/G' once and for all and let $C'(n, p)$ be a positive number such that ${}^tU_iU_i > C'(n, p)1_n$ for all i. Without loss of generality we may assume that T_0 is reduced in the sense of Minkowski and hence, as is well known, $T_0 > C_n(\min T_0)1_n$ holds for some absolute constant C_n. Since $(nT_0)Z_p = 2Z_p$, we can choose $V \in SL(n, Z_p)$ so that $T_0[V] = \begin{pmatrix} T_1 & 0 \\ 0 & * \end{pmatrix}$ where

$$T_1 = \begin{pmatrix} 2h & 0 \\ 0 & 2k \end{pmatrix} \quad h \in Z_p^\times,\ k \in Z_p\,,$$

$$\begin{pmatrix} 2h & k \\ k & 2hk^2 \end{pmatrix} = \begin{pmatrix} 2h & 1 \\ 1 & 2h \end{pmatrix}\left[\begin{pmatrix} 1 & 0 \\ 0 & k \end{pmatrix}\right] \quad h = 0, 1,\ k \in Z_p^\times \quad \text{if } p = 2\,,$$

or

$$\begin{pmatrix} 2h & 0 & 0 \\ 0 & & \\ 0 & \multicolumn{2}{c}{2^i\begin{pmatrix} 2k & 1 \\ 1 & 2k \end{pmatrix}} \end{pmatrix} \quad h \in Z_p^\times,\ k = 0, 1,\ i \geq 2 \quad \text{if } p = 2\,.$$

Take a representative $U = U_i$ of G/G' so that $U \equiv V \bmod 8pZ_p$; then we have $T_0[U] > C_n(\min T_0)1_n[U] > C_nC'(n, p)(\min T_0)1_n$, and putting $A = \begin{pmatrix} \begin{pmatrix} 1 & u \\ 0 & p^b \end{pmatrix} & \\ & 1_{n-2} \end{pmatrix}$ and hence

$$p^bA^{-1} = \begin{pmatrix} \begin{pmatrix} p^b & -u \\ 0 & 1 \end{pmatrix} & \\ & p^b1_{n-2} \end{pmatrix},$$

we have

$$\begin{aligned} \min T[UA^{-1}] &= \min p^{2b+c}T_0[UA^{-1}] \\ &> C_nC'(n, p)p^c(\min T_0) \min (1_n[p^bA^{-1}]) \\ &= C_nC'(n, p)p^c(\min T_0) \min \{(p^bx - uy)^2 + y^2, p^{2b}\} \end{aligned}$$

where x, y run over integers not all zero, and by Lemma 1

$$> C_n C'(n, p) p^c (\min T_0) p^b / 16$$

if $\sqrt{p^b}/4 < u < \sqrt{p^b}$.

Putting $H = AU^{-1}$, $C(n, p) = C_n C'(n, p)/16$, we have

$$\min T[H^{-1}] > C(n, p) p^{b+c} \min T_0 .$$

Since $T[H^{-1}] = p^c T_0[U][p^b A^{-1}]$ and $nT_0 \subset 2Z$, we have $nT[H^{-1}] \subset 2p^c Z \subset 2Z$. The (2, 2) entry of $T[H^{-1}]$ is equal mod $8p^{1+c}Z_p$ to

$$2p^c(hu^2 + k), \quad 2p^c(hu^2 - ku + hk^2), \quad 2p^c(hu^2 + 2^t k)$$

according to the order of above canonical forms of T_1 and hence to complete the proof, it is enough to show that they are not zero modulo $8p^{1+c}$ for some u with $\sqrt{p^b}/4 < u < \sqrt{p^b}$. Noting $\sqrt{p^b} - \sqrt{p^b}/4 > 4$ because of $p^b \geq 36$, we have only to choose $u \in Z$ with $\sqrt{p^b}/4 < u < \sqrt{p^b}$ so that $(u, p) = 1$ if $k \in pZ_p$, and $hu^2 + k \not\equiv 0 \bmod p$ if $k \in Z_p^\times$ in the left case; $2 \nmid u$ if $h = 0$, and $2 | u$ if $h = 1$ in the middle case: $2 \nmid u$ in the right case. Thus we have proved Lemma 2.

Remark. In the above proof, all but (2, 2) entries of $T[H^{-1}]$ are divided by p^{b+c}, and if T_1 is of the first canonical form, then $T[H^{-1}]$ represents $2p^c h = p^{-2b} \times (1, 1)$ entry of $T[V]$ over Z_p if either $p \neq 2$, $k \in pZ_p$ or $p = 2$, $k \in 8Z_2$.

Proof of Theorem. First we note that for a positive lattice $K' \supset K$, $\min K' \geq [K' : K]^{-2} \min K$ holds, since $[K' : K]K' \subset K$ implies $\min [K' : K]K' \geq \min K$. Let M, N be those in Theorem. If a prime p does not divide dM, then $Z_p M$ is unimodular and $nZ_p M = 2Z_p$. Hence Z_p contains a submodule isometric to $\perp_n \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle$ as an orthogonal component. Therefore $Z_p N$ is primitively represented $Z_p M$. If $p | dM$ and $\operatorname{ind} Q_p M \geq n$, then by virtue of Theorem 2 in [4] there is an isometry u from $Z_p N$ to $Z_p M$ such that $[Q_p u(Z_p N) \cap Z_p M_p : u(Z_p N)]$ is bounded by a number C_p dependent only on $Z_p M$. Hence $\bar{N}_p = u^{-1}(Q_p u(Z_p N) \cap Z_p M)$ $(\supset Z_p N)$ is primitively represented by $Z_p M$, and enlarging N to N'' so that $Z_p N'' = \bar{N}_p$, $Z_p N''$ is primitively represented by $Z_p M$ and $\min N'' \geq C_p^{-2} \min N$. Suppose that $p | dM$ and $\operatorname{ind} Q_p M = n - 1$. We fix a $2p^{k_p} Z_p$-maximal sublattice K of $Z_p M$ for some k_p once and for all. If $nZ_p N \supset 2p^{2+k_p} Z_p$, then there is an isometry u from $Z_p N$ to $Z_p M$ such that $[Q_p u(Z_p N) \cap Z_p M : u(Z_p N)]$ is bounded by a number C_p dependent only on k_p and $Z_p M$, applying the theorem referred above where N_1 there, should be the first Jordan component of $Z_p N$, and nothing that the number of distinct

https://doi.org/10.1017/S0027763000001501 Published online by Cambridge University Press

isometry classes by $O(Z_pM)$ of modular submodules of Z_pM with $n \supset 2p^{2+k_p}Z_p$ is finite. In this case we have obtained an enlarged quadratic lattice of N at p which contains N with index dependent only on k_p and Z_pM and is primitively represented by M over Z_p. Finally we deal with the case that $p \mid dM$, $\operatorname{ind} Q_pM = n - 1$ and $nZ_pN \subset 2p^{2+k_p}Z_p$. Put $N = \langle p^{2b+c+k_p}T_0 \rangle$ where $0 < b \in Z$, $c = 0, 1$ and $nT_0 \subset 2Z$, $(nT_0)Z_p = 2Z_p$. By virtue of Lemma 2, there exists a matrix H in $M_n(Z)$ such that $\det H$ is a power of p,

$$\min p^{2b+c}T_0[H^{-1}] > C(n, p)p^{b+c} \min T_0 ,$$
$$p^{2b+c}T_0[H^{-1}] \not\equiv 0 \bmod 8p^{1+c} \quad \text{and} \quad n(p^{2b+c}T_0[H^{-1}]) \subset 2Z .$$

Taking a quadratic lattice N' $(\supset N)$ corresponding to H, N' satisfies $n(Z_pN') \subset 2p^{k_p}Z_p = nK$, $n(Z_pN') \not\subset 8p^{1+c+k_p}Z_p$ and $\min N' > C(n, p)p^{b+c+k_p}$ $\min T_0 \geq C(n, p)p^{(2b+c+k_p)/2} \min T_0 = C(n, p)p^{-(\operatorname{ord}_p q_0)/2} \min N$. Since $Q_pN' = Q_pN$ is represented by $Q_pM = Q_pK$, Z_pN' is represented by the maximal lattice K and hence by Z_pM. Applying the argument in the case of $p \mid 2dM$, $nZ_pN \supset 2p^{2+k_p}Z_p$ to N', M, noting $n(Z_pN') \not\subset 8p^{1+c+k_p}Z_p$, there is a lattice N'' $(\supset N')$ such that $[N'' : N']$ is a power of p bounded by a number dependent on k_p and Z_pM, and Z_pN'' is primitively represented by Z_pM. Iterating the construction of N'' for primes p dividing dM, we complete the proof of Theorem. ■

Remark. Let us consider the case $m = 2n + 1$. Let M be a positive lattice of $\operatorname{rk} M = m$ and N a positive lattice of $\operatorname{rk} N = n$ which is represented by $\operatorname{gen} M$. It is easy to see that the assertion similar to Theorem holds, using Lemma 2 and its remark, provided that for every prime p for which $\operatorname{ind} Q_pM = n - 1$ holds and Z_pN has a Jordan splitting $Z_pN = \langle a \rangle \perp N_1$ where $\operatorname{ord}_p a$ is bounded but $\operatorname{ord}_p nN_1$ is large, there is a lattice $\overline{N}$ such that $[\overline{N} : N]$ is a power of p, $Z_p\overline{N}$ is represented by Z_pM, $Z_p\overline{N}$ contains a binary lattice B with $\operatorname{ord}_p dB$ bounded and $\min \overline{N}$ is large.

This condition is not necessarily satisfied for $n = 2$ as follows: For $N = \langle a \rangle \perp \langle p^r \rangle$ with $(a, p) = 1$, $\overline{N} = \langle a \rangle \perp \langle p^{r-2t} \rangle$ holds if $[\overline{N} : N] = p^t$. Thus $\min \overline{N}$ is small if $\operatorname{ord}_p \overline{N}$ is small. This leads us to a falsehood of the assertion $(A)_{m,n}$ when $m = 2n + 1 = n + 3$, $n = 2$, as in [2].

§ 2.

We have observed that it is important whether for a given sequence $\{N_t\}$ of positive lattices represented by $\operatorname{gen} M$ with $\min N_t \to \infty$, there is

https://doi.org/10.1017/S0027763000001501 Published online by Cambridge University Press

a lattice $\overline{N}_t$ with $\min \overline{N}_t$ large which contains N_t and is primitively represented at every spot by $\operatorname{gen} M$ or not. If there is no such $\overline{N}_t$, then we must deduce a falsehood of the assertion $(A)_{m,n}$.

In this section we show that it is hard to construct such a sequence by scalings of a fixed lattice by giving the following

PROPOSITION. *Let M, N be positive lattices of $\operatorname{rk} M = m \geq \operatorname{rk} N + 3$, $\operatorname{rk} N = n \geq 3$. We fix representatives $\{N_i\}$ of classes in the genus of N once and for all, and take a finite set S ($\ni 2$) of primes such that if $p \notin S$, then $Z_p N_i = Z_p N$ holds for all i and $Z_p M$, $Z_p N$ are unimodular. For any given number C_1, there is a positive number $C_2 = C_2(C_1, M, N)$ such that if a natural number a ($\geq C_2$) is not divided by any prime in S and the scaling $N(a)$ of N by a is locally represented by M, then there is a lattice $\overline{N}_a$ with $\min \overline{N}_a \geq C_1$ which contains $N(a)$ and $Z_p \overline{N}_a$ is primitively represented by $Z_p M$ for every prime p.*

COROLLARY. *For the above special sequence $\{N(a)\}$, the assertion $(APW)_{m,n}$ implies the assertion $(A)_{m,n}$.*

This follows trivially and to prove Proposition, we must prepare the following

THEOREM. *Let L be a positive lattice of $nL = 2Z$ and $\operatorname{rk} L = m \geq 2$. For a prime p we define an integer a_p by the following:*

If $m \geq 3$ and the Jordan splitting is of form

$$Z_p L = \langle 2\varepsilon_1 \rangle \perp \langle 2\varepsilon_2 p^{a_p} \rangle \perp \cdots \qquad p \geq 2\,,$$

or

$$\langle 2\varepsilon_1 \rangle \perp \left\langle 2^{a_2} \begin{pmatrix} 2c & 1 \\ 1 & 2c \end{pmatrix} \right\rangle \perp \cdots \qquad p = 2\,,$$

where $\varepsilon_1, \varepsilon_2 \in Z_p^\times$ and $c = 0$ or 1, then a_p is given as in the above, otherwise $a_p = 0$. Then there is a lattice M in the genus of L such that

$$\min M \gg (dL)^{1/m - \varepsilon} \Big(\prod_{p \mid 2dL} p^{a_p} \Big)^{-1/m}$$

where ε is any positive number and $A \gg B$ means $A > cB$ for a constant c dependent only on ε and m.

Remark. $\min L \ll (dL)^{1/m}$ is well known.

Before the proof of Theorem we show that Proposition follows from Theorem.

Let M, N, N_i, S be those in Proposition. For a prime p, let $K = Z_p[e, f]$ be a quadratic lattice over Z_p defined by $Q(e) = Q(f) = 0$, $B(e, f) = a$. Then $\bar{K} = Z_p[a^{-1}e, f] = \left\langle\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\right\rangle$ is clear. Hence for a prime p dividing a we can take a lattice $\bar{N}_p$ which contains $Z_pN(a)$ and is isometric to an orthogonal sum of a unimodular lattice of $\mathrm{rk} = n-1$ or $n-2$ and an aZ_p-modular lattice of $\mathrm{rk} = 1$ or 2, enlarging binary hyperbolic aZ_p-modular lattices to unimodular lattices as above. Let N' be a lattice which is isometric to $\bar{N}_p$ for $p|a$ and to $Z_pN(a)$ for $p \nmid a$ and has a large minimum by virtue of Theorem. Since there is an isometry from $Z_pN(a)$ to Z_pN' for every prime and $QN(a) = QN'$, N' contains a lattice which is isometric to $N_i(a)$ for some i. Pulling back N', there is a lattice N'' such that $\min N''$ is large, $N'' \supset N_i(a)$, $Z_pN'' = Z_pN_i(a)$ for $p \nmid a$ and Z_pN'' has a unimodular component of $\mathrm{rk} = n-1$ or $n-2$ for $p|a$. Define a new lattice $\bar{N}$ by $Z_p\bar{N} = Z_pN(a)$ for $p \nmid a$ and $Z_p\bar{N} = Z_pN''$ for $p|a$. By definition $\bar{N}$ contains $N(a)$ and $Z_p\bar{N} = Z_pN''$ if $p \notin S$ and $p \nmid a$. Since

$$[\bar{N}: \bar{N} \cap N''] = \prod [Z_p\bar{N}: Z_p\bar{N} \cap Z_pN''] = \prod_{p\in S} [Z_p\bar{N}: Z_p\bar{N} \cap Z_pN'']$$
$$= \prod_{p\in S} [Z_pN(a): Z_pN(a) \cap Z_pN_i(a)] = [N: N \cap N_i]$$

and $[\bar{N}: \bar{N} \cap N'']^2 \min \bar{N} \geq \min(\bar{N} \cap N'')$, we have $\min \bar{N} \geq [N: N \cap N_i]^{-2} \times \min(\bar{N} \cap N'') \geq [N: N \cap N_i]^{-2} \min N''$. Thus we have constructed a lattice $\bar{N}$ which contains $N(a)$, has a large minimum and satisfies that $Z_p\bar{N} = Z_pN(a)$ for $p \nmid a$ and $Z_p\bar{N}$ has a unimodular component of $\mathrm{rk} = n-1$ or $n-2$ for $p|a$. By assumption, $N(a)$ is represented by M locally and Z_pN, Z_pM are unimodular if $p \notin S$. Hence $Z_p\bar{N}$ is primitively represented by Z_pM if $p \notin S$ and $p \nmid a$. If $p|a$, then by cancellation of a unimodular component of Z_pN from $Z_p\bar{N}$ and Z_pM, the remaining part of $Z_p\bar{N}$ is primitively represented by the one of Z_pM and hence $Z_p\bar{N}$ is primitively represented by Z_pM. Enlarging $\bar{N}$ for every prime $p \in S$ we get a lattice $\bar{N}_a$ which contains $N(a)$, is primitively represented by M locally and has a large minimum since $[\bar{N}_a: \bar{N}] = \prod_{p\in S} [Z_p\bar{N}_a: Z_pN(a)]$ is bounded by a number depending on N and M. Thus we have completed the proof of Proposition, assuming Theorem.

Proof of Theorem. We divide the proof to two cases $m = 2$ and $m \geq 3$. First we treat the case $m = 2$.

LEMMA. *For given natural numbers a and D, the number of b, c*

https://doi.org/10.1017/S0027763000001501 Published online by Cambridge University Press

which satisfy $0 \leq b \leq a \leq c$ *and* $D = 4ac - b^2$, *is* $O(a^{\varepsilon}(D, a)^{1/2})$ *where* ε *is any positive number.*

Proof. The number of b, c is less than or equal to $\#\{b \bmod 4a \mid b^2 \equiv -D \bmod 4a\}$. First we show, for a prime power p^n, $\#\{x \bmod p^n \mid x^2 \equiv -D \bmod p^n\} \leq 4(D, p^n)^{1/2}$. Put $d = \operatorname{ord}_p D$. If $d \geq n$, then $\#\{x \bmod p^n \mid x^2 \equiv -D \bmod p^n\} = \#\{x \bmod p^n \mid x^2 \equiv 0 \bmod p^n\} = p^{[n/2]} < 4(D, p^n)^{1/2}$ holds, where $[r]$ means the largest integer which does not exceed r. Suppose $d < n$. If $x^2 \equiv -D \bmod p^n$, then d is even and $x = p^{d/2}y$ for an integer y satisfying $y^2 \equiv -Dp^{-d} \bmod p^{n-d}$. The number of solutions modulo p^{n-d} for $y^2 \equiv -Dp^{-d} \bmod p^{n-d}$ is at most four, and for each y, $x = p^{d/2}(y + p^{n-d}z)$ ($z \bmod p^{d/2}$) is a solution. This completes the above inequality. Hence $\#\{b \bmod 4a \mid b^2 \equiv -D \bmod 4a\} \leq (\prod_{p \mid 4a} 4)(D, 4a)^{1/2} \ll a^{\varepsilon}(D, a)^{1/2}$. ■

Let L be a binary positive lattice with $nL = 2Z$, $dL = D$, and denote by h the number of isometry classes in $\operatorname{gen} L$. Every binary even positive lattice corresponds to the only one reduced matrix $\begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}$ $0 \leq b \leq a \leq c$. Hence we have

$$\begin{aligned} &\sum_{a=1}^{k} \#\{M \in \operatorname{gen} L/\mathrm{cls} \mid \min M = 2a\} \\ &\ll \sum_{a=1}^{k} a^{\varepsilon}(D, a)^{1/2} \\ &\ll \sum_{s \mid D} \sum_{1 \leq t \leq k/s} (st)^{\varepsilon} s^{1/2} \\ &\ll \sum_{s \mid D} s^{1/2+\varepsilon}(k/s)^{1+\varepsilon} \\ &= k^{1+\varepsilon} \sum_{s \mid D} s^{-1/2} \ll k^{1+\varepsilon} D^{\varepsilon} . \end{aligned}$$

Thus there is a number c dependent only on ε so that

$$\sum_{a=1}^{k} \#\{M \in \operatorname{gen} L/\mathrm{cls} \mid \min M = 2a\} < ck^{1+\varepsilon} D^{\varepsilon} .$$

If the class number h of $\operatorname{gen} L$ is greater than $ck^{1+\varepsilon}D^{\varepsilon}$, then there is a lattice $M \in \operatorname{gen} L$ such that $\min M > k$. By Siegel, $h \gg D^{1/2-\varepsilon}$ is well known. Noting that ε's are any positive numbers, we have $\min M \gg D^{1/2-\varepsilon}$ for any $\varepsilon > 0$, which completes the proof in the case $m = 2$.

To treat the case $m \geq 3$, we prepare several lemmas. Let us denote by p a prime number.

LEMMA 1. *Let* a *and* b *be integers and* $a \geq b \geq 0$. *For* $\alpha \in Z_p$ *with*

https://doi.org/10.1017/S0027763000001501 Published online by Cambridge University Press

$\operatorname{ord}_p \alpha = b$, *the number* t *of solutions modulo* p^a *of* $x^2 \equiv \alpha \bmod p^a$ *is* $O(p^{b/2})$.

Proof. Suppose $a = b$; then t is equal to $\#\{x \bmod p^a \mid x^2 \equiv 0 \bmod p^a\} = p^{[a/2]} \leq p^{b/2}$. Suppose $a > b$. If b is odd, then there is no solution and hence $t = 0$. If b is even and $b = 2d$, then t is equal to

$$\begin{aligned}&\#\{y \bmod p^{a-d} \mid y^2 \equiv \alpha p^{-2d} \bmod p^{a-2d}\} \\ &= p^d \#\{y \bmod p^{a-2d} \mid y^2 \equiv \alpha p^{-2d} \bmod p^{a-2d}\} \\ &\leq 4p^d = O(p^{b/2}) . \qquad \blacksquare\end{aligned}$$

LEMMA 2. *For* $0 \leq a \leq h-1$, $\varepsilon \in \boldsymbol{Z}_p^\times$ *and* $\alpha \in \boldsymbol{Z}_p$, *we put* $t = \#\{x \bmod p^h, y \bmod p^{h-a} \mid x^2 + \varepsilon p^a y^2 \equiv \alpha \bmod p^h, (x, y) = 1\}$. *Then* $t = O(p^{h-a/2})$ *holds.*

Proof. Let t_1 (resp. t_2) be the number of solutions under an additional condition $p \mid y$ (resp. $p \nmid y$). $t = t_1 + t_2$ is clear. Without loss of generality we may put $\alpha = \delta p^c$, $\delta \in \boldsymbol{Z}_p^\times$, $0 \leq c \leq h$. Then t_1 is equal to

$$\#\{x \bmod p^h,\ y \bmod p^{h-a-1} \mid x^2 + \varepsilon p^{a+2} y^2 \equiv \alpha \bmod p^h,\ p \nmid x\} .$$

If $c > 0$ i.e., $p \mid \alpha$, then $t_1 = 0$ holds. If $c = 0$, then $\alpha - \varepsilon p^{a+2} y^2$ is in $\boldsymbol{Z}_p^\times$ and hence $t_1 = O(p^{h-a-1}) = O(p^{h-a/2})$. t_2 is equal to

$$\begin{aligned}&\sum_{\substack{x \bmod p^h \\ x^2 \equiv \delta p^c \bmod p^a}} \#\{y \bmod p^{h-a} \mid \varepsilon p^a y^2 \equiv \delta p^c - x^2 \bmod p^h,\ p \nmid y\} . \\ &= \sum_{\substack{x \bmod p^h \\ x^2 \equiv \delta p^c \bmod p^a}} \#\{y \bmod p^{h-a} \mid y^2 \equiv (\varepsilon p^a)^{-1}(\delta p^c - x^2) \bmod p^{h-a},\ p \nmid y\} \\ &\ll \#\{x \bmod p^h \mid \operatorname{ord}_p (x^2 - \delta p^c) = a\} .\end{aligned}$$

We show that this is $O(p^{h-a/2})$ in each case of $c \geq a$, $c < a$. Suppose $c \geq a$; then $t_2 \ll \#\{x \bmod p^h \mid x^2 \equiv 0 \bmod p^a\} = p^{h-[(a+1)/2]} \leq p^{h-a/2}$. Suppose $c < a$. If $x^2 - \delta p^c \equiv 0 \bmod p^a$ is soluble, then $2 \mid c$ and $x = p^{c/2} z$ for some $z \in \boldsymbol{Z}_p$. Hence t_2 is less than

$$\begin{aligned}&\#\{z \bmod p^{h-c/2} \mid \operatorname{ord}_p (p^c(z^2 - \delta)) = a\} \\ &\leq \#\{z \bmod p^{h-c/2} \mid z^2 \equiv \delta \bmod p^{a-c}\} \\ &= p^{h-c/2-(a-c)} \#\{z \bmod p^{a-c} \mid z^2 \equiv \delta \bmod p^{a-c}\} \\ &= O(p^{h-a+c/2}) = O(p^{h-a/2}) .\end{aligned}$$

Thus we have completed the proof. $\blacksquare$

LEMMA 3. *For integers* a, c *and* h *satisfying* $0 \leq a \leq h-1$ *and* $0 \leq c \leq h$ *and for* ε, $\delta \in \boldsymbol{Z}_p^\times$, *we put*

$$t = \#\{x \bmod p^h,\ y \bmod p^{h-a} \mid x^2 + \varepsilon p^a y^2 \equiv \delta p^c \bmod p^h\}.$$

Then we have $t = O(hp^{h-a/2})$.

Proof. t is equal to

$$\sum_{0 \le i \le h-a} \#\{x \bmod p^h,\ y \bmod p^{h-a} \mid x^2 + \varepsilon p^a y^2 \equiv \delta p^c \bmod p^h,\ (x, y) = p^i\}$$
$$= t_1 + t_2 + t_3,$$

where t_1, t_2 and t_3 are partial sums under conditions $2i < c$, $2i = c$ and $2i > c$ respectively. Further we divide t_1 to the sum of $t_{1,1}$ and $t_{1,2}$ where $t_{1,1}$, $t_{1,2}$ are partial sums under conditions $i < (h-a)/2$, $i \ge (h-a)/2$ respectively. $t_{1,1}$ is equal to

$$\sum_{\substack{0 \le i < (h-a)/2 \\ i < c/2}} \#\{x \bmod p^{h-i},\ y \bmod p^{h-a-i} \mid x^2 + \varepsilon p^a y^2 \equiv \delta p^{c-2i} \bmod p^{h-2i},\ (x, y) = 1\}$$

and considering $x \bmod p^{h-2i}$, $y \bmod p^{h-a-2i}$ and using Lemma 2 we have $t_{1,1} \ll \sum_{\substack{0 \le i < (h-a)/2 \\ i < c/2}} p^{2i+(h-2i-a/2)} < hp^{h-a/2}$. $t_{1,2}$ is equal to

$$\sum_{\substack{(h-a)/2 \le i \le h-a \\ i < c/2}} \#\{x \bmod p^{h-i},\ y \bmod p^{h-a-i} \mid x^2 + \varepsilon p^a y^2 \equiv \delta p^{c-2i} \bmod p^{h-2i},\ (x, y) = 1\}$$
$$\le \sum_{(h-a)/2 \le i < c/2} \#\{x \bmod p^{h-i},\ y \bmod p^{h-a-i} \mid x^2 \equiv \delta p^{c-2i} \bmod p^{h-2i},\ (x, y) = 1\}$$

because of $h - 2i \le a$,

$$< \sum_{(h-a)/2 \le i < c/2} p^{h-a-i}\, \#\{x \bmod p^{h-i} \mid x^2 \equiv \delta p^{c-2i} \bmod p^{h-2i}\}$$
$$= \sum_{(h-a)/2 \le i < c/2} p^{h-a}\, \#\{x \bmod p^{h-2i} \mid x^2 \equiv \delta p^{c-2i} \bmod p^{h-2i}\}$$
$$\ll p^{h-a} \sum_{(h-a)/2 \le i < c/2} p^{(c-2i)/2} \qquad \text{(by Lemma 1)}$$
$$< p^{h-a+c/2} \sum_{(h-a)/2 \le i} p^{-i}$$
$$\ll p^{h-a+c/2-(h-a)/2} \le p^{h-a/2}.$$

Since t_2 is zero if $2 \nmid c$, we may assume $2 \mid c$ and hence we have $0 \le c/2 \le h - a$. t_2 is equal to

$$\#\{x \bmod p^{h-c/2},\ y \bmod p^{h-a-c/2} \mid x^2 + \varepsilon p^a y^2 \equiv \delta \bmod p^{h-c},\ (x, y) = 1\}$$
$$= p^{c/2}\, \#\{x \bmod p^{h-c},\ y \bmod p^{h-a-c/2} \mid x^2 + \varepsilon p^a y^2 \equiv \delta \bmod p^{h-c},\ (x, y) = 1\}.$$

If $a = 0$, then t_2 is equal to

$$p^c\, \#\{x, y \bmod p^{h-c} \mid x^2 + \varepsilon y^2 \equiv \delta \bmod p^{h-c},\ (x, y) = 1\}$$
$$\ll p^h \qquad \text{(by Lemma 2)} \qquad = p^{h-a/2}.$$

If $a > 0$, then t_2 is less than or equal to

$$\begin{aligned} & p^{c/2} \sum_{y \bmod p^{h-a-c/2}} \#\{x \bmod p^{h-c} \mid x^2 \equiv \delta - \varepsilon p^a y^2 \bmod p^{h-c}\} \\ & \ll p^{c/2+h-a-c/2} \qquad \text{(by Lemma 1)} \\ & < p^{h-a/2} . \end{aligned}$$

If $c < h$, then t_3 is equal to 0, and hence we may put $c = h$. Then t_3 is equal to

$$\begin{aligned} & \sum_{h/2 < i \leq h-a} \#\{x \bmod p^h,\ y \bmod p^{h-a} \mid (x, y) = p^i\} \\ & < \sum_{i > h/2} p^{(h-i)+(h-a-i)} \ll p^{2h-a-h} < p^{h-a/2} . \end{aligned}$$

Summing up, we complete the proof. ∎

LEMMA 4. *Put* $t = \#\{x, y \bmod 2^h \mid xy \equiv a \bmod 2^h\}$ *for an integer* a. *Then* $t \ll h \cdot 2^h$ *holds.*

Proof. t is equal to

$$\begin{aligned} & \sum_{0 \leq i \leq h} \#\{x \bmod 2^{h-i},\ y \bmod 2^h \mid 2^i xy \equiv a \bmod 2^h,\ 2 \nmid x\} \\ & = \sum_{0 \leq i \leq h} \varphi(2^{h-i}) \#\{y \bmod 2^h \mid 2^i y \equiv a \bmod 2^h\} , \end{aligned}$$

where φ means the Euler's function

$$< \sum_{0 \leq i \leq h} 2^{h-i} \cdot 2^i \leq (h+1)2^h \ll h \cdot 2^h .$$ ∎

LEMMA 5. *Put* $t = \#\{x, y \bmod 2^h \mid x^2 + xy + y^2 \equiv a \bmod 2^h\}$ *for an integer* a. *Then* $t \ll 2^h$ *holds.*

Proof. Put $a = b \cdot 2^c$, $2 \nmid b$, and note that $x^2 + xy + y^2 \equiv 0 \bmod 2^n$ implies $x^2 \equiv y^2 \equiv 0 \bmod 2^n$. If $c \geq h$, then t is equal to

$$\begin{aligned} & \#\{x, y \bmod 2^h \mid x^2 + xy + y^2 \equiv 0 \bmod 2^h\} \\ & \leq \#\{x, y \bmod 2^h \mid x^2 \equiv y^2 \equiv 0 \bmod 2^h\} \\ & \ll 2^h . \end{aligned}$$

If $c < h$ and $2 \nmid c$, then we have $t = 0$. Suppose $c < h$ and $2 \mid c$; then t is equal to

$$\begin{aligned} & \#\{x, y \bmod 2^{h-c/2} \mid x^2 + xy + y^2 \equiv b \bmod 2^{h-c}\} \\ & = 2^c \#\{x, y \bmod 2^{h-c} \mid x^2 + xy + y^2 \equiv b \bmod 2^{h-c}\} \\ & \leq 2^{c+1} \#\{x, y \bmod 2^{h-c} \mid x^2 + xy + y^2 \equiv b \bmod 2^{h-c},\ 2 \nmid y\} . \end{aligned}$$

Here we claim that there is at most 2 solutions of x for $x^2 + xy + y^2 \equiv b \bmod 2^{h-c}$ for an odd y. Suppose that x_1, x_2 are solutions. Then $(x_1 - x_2)(x_1 + x_2 + y) \equiv 0 \bmod 2^{h-c}$ holds. Since only one of $x_1 - x_2$, $x_1 + x_2 + y$ is odd, only one of $x_1 - x_2 \equiv 0 \bmod 2^{h-c}$ or $x_1 + x_2 + y \equiv 0 \bmod 2^{h-c}$ can occur, and hence the number of solutions is at most 2. Thus $t \leq 2^{c+2}\varphi(2^{h-c}) \ll 2^h$ holds. ■

LEMMA 6. *For $h > a \geq 1$ put*

$$t = \#\{x \bmod 2^{h-1},\ y, z \bmod 2^{h-a} \mid 2x^2 + 2^{a+1}yz \equiv b \bmod 2^{h+1}\}$$

for an integer b. Then $t \ll h \cdot 2^{2h-3a/2}$ holds.

Proof. If b is odd, then t is clearly zero, and hence we may put $b = d \cdot 2^{c+1}$, $2 \nmid d$, $c \geq 0$. Then t is equal to

$$\begin{aligned}
&\sum_{x \bmod 2^{h-1}} \#\{y, z \bmod 2^{h-a} \mid 2^a yz \equiv d \cdot 2^c - x^2 \bmod 2^h\} \\
&= \sum_{\substack{x \bmod 2^{h-1} \\ x^2 \equiv d \cdot 2^c \bmod 2^a}} \#\{y, z \bmod 2^{h-a} \mid yz \equiv 2^{-a}(d \cdot 2^c - x^2) \bmod 2^{h-a}\} \\
&\ll (h-a)2^{h-a} \#\{x \bmod 2^{h-1} \mid x^2 \equiv d \cdot 2^c \bmod 2^a\} \qquad \text{(by Lemma 4)} \\
&< h \cdot 2^{2(h-a)} \#\{x \bmod 2^a \mid x^2 \equiv d \cdot 2^c \bmod 2^a\} \\
&\ll h \cdot 2^{2(h-a)+\min(c,a)/2} \qquad \text{(by Lemma 1)} \\
&< h \cdot 2^{2h-3a/2}.
\end{aligned}$$

■

LEMMA 7. *For $h > a \geq 1$ put*

$$t = \#\{x \bmod 2^{h-1},\ y, z \bmod 2^{h-a} \mid 2x^2 + 2^{a+1}(y^2 + yz + z^2) \equiv b \bmod 2^{h+1}\}.$$

Then we have $t \ll 2^{2h-3a/2}$.

Proof. Put $b = d \cdot 2^{c+1}$, $2 \nmid d$, $c \geq 0$; then t is equal to

$$\begin{aligned}
&\sum_{\substack{x \bmod 2^{h-1} \\ x^2 \equiv d \cdot 2^c \bmod 2^a}} \#\{y, z \bmod 2^{h-a} \mid y^2 + yz + z^2 \equiv 2^{-a}(d \cdot 2^c - x^2) \bmod 2^{h-a}\} \\
&\ll 2^{h-a} \#\{x \bmod 2^{h-1} \mid x^2 \equiv d \cdot 2^c \bmod 2^a\} \qquad \text{(by Lemma 5)} \\
&\ll 2^{2(h-a)} \#\{x \bmod 2^a \mid x^2 \equiv d \cdot 2^c \bmod 2^a\} \\
&\ll 2^{2h-3a/2}
\end{aligned}$$

as in the proof of Lemma 6. ■

Recall that L is a positive lattice of $nL = 2Z$, $\operatorname{rk} L = m \geq 3$.

LEMMA 8. *We have $\prod_{p \nmid 2dL} \alpha_p(t, L) \ll (tdL)^\varepsilon$ for a natural number t and any positive number ε where α_p is the local density.*

https://doi.org/10.1017/S0027763000001501 Published online by Cambridge University Press

Proof. For a prime number p not dividing $2dL$ we put $\delta = \delta_p = \chi((-1)^{m/2}dL)$ (resp. $\chi((-1)^{(m-1)/2}tp^{-e}dL)$, $r = r_p = p^{1-m/2}$ (resp. p^{2-m}) for $2\mid m$ (resp. $2\nmid m$), where χ is the quadratic residue symbol for p and $e = e_p = \operatorname{ord}_p t$.

By Hilfssatz 16 in [9], $\alpha_p(t, L)$ is equal to

$$\begin{array}{ll} (1-\delta p^{-m/2})(1+\delta r+\cdots+(\delta r)^e) & 2\mid m\,, \\ (1-p^{1-m})(1+r+\cdots+r^{(e-1)/2}) & 2\nmid e,\ 2\nmid m\,, \\ (1-p^{1-m})\{1+r+\cdots+r^{e/2-1}+r^{e/2}(1-\delta p^{(1-m)/2})^{-1}\} & 2\mid e,\ 2\nmid m\,. \end{array}$$

If m is even, then we have

$$\begin{aligned} \alpha_p(t, L) &\leq (1+p^{-m/2})\sum_{k\geq 0} r^k \\ &= (1+p^{-m/2})(1-p^{1-m/2})^{-1}\,. \end{aligned}$$

Hence for an even integer m (≥ 3) we have

$$\begin{aligned} \prod_{p\nmid 2dL}\alpha_p(t, L) &< \prod_{p\nmid 2dL}(1+p^{-m/2})\prod_{p\mid t}(1-p^{1-m/2})^{-1} \\ &\ll \prod_{p\mid t}(1-p^{1-m/2})^{-1} \leq \prod_{p\mid t}(1-p^{-1})^{-1} \ll t^{\varepsilon} \end{aligned}$$

for any positive ε, since $\varphi(t) > ct(\log\log t)^{-1}$ for $t \geq 3$ and some positive number c.

Suppose $2\nmid m$. If $2\nmid e$, then we have

$$\begin{aligned} \alpha_p(t, L) &= (1-p^{1-m})(1-p^{(2-m)(e+1)/2})(1-p^{2-m})^{-1} \\ &< (1-p^{2-m})^{-1} < (1-p^{2-m})^{-1}(1-p^{(1-m)/2})^{-1}\,. \end{aligned}$$

If $e = 0$, then we have $\alpha_p(t, L) < (1-\delta p^{(1-m)/2})^{-1}$.

Suppose $2\mid e$, $e > 0$; then $\alpha_p(t, L)$ is less than or equal to

$$\begin{aligned} &(1-p^{1-m})(1-p^{(2-m)e/2})(1-p^{2-m})^{-1} \\ &\qquad + p^{(2-m)e/2}(1-p^{1-m})(1-p^{(1-m)/2})^{-1} \\ &\quad = (1-p^{1-m})(1-p^{2-m})^{-1}(1-p^{(1-m)/2})^{-1} \\ &\qquad \times\{1-p^{(1-m)/2}+p^{(1-m)/2+(2-m)e/2}-p^{(2-m)(e/2+1)}\} \\ &\quad < (1-p^{1-m})(1-p^{2-m})^{-1}(1-p^{(1-m)/2})^{-1}(1-p^{(2-m)(e/2+1)}) \\ &\quad < (1-p^{2-m})^{-1}(1-p^{(1-m)/2})^{-1}\,. \end{aligned}$$

Thus we have, for odd m

$$\prod_{p\nmid 2dL}\alpha_p(t, L) < \prod_{p\nmid 2tdL}(1-\delta_p p^{(1-m)/2})^{-1}\cdot\prod_{p\mid t}(1-p^{2-m})^{-1}(1-p^{(1-m)/2})^{-1}\,.$$

Therefore for odd $m \geq 5$ we have $\prod_{p\nmid 2dL}\alpha_p(t, L) \ll 1$, and for $m = 3$,

https://doi.org/10.1017/S0027763000001501 Published online by Cambridge University Press

$$\prod_{p\nmid 2dL}\alpha_p(t, L) < \prod_{p\nmid 2tdL}(1-\delta_p p^{-1})^{-1}\cdot \prod_{p\mid t}(1-p^{-1})^{-2}$$
$$\ll (tdL)^{\varepsilon}\,,$$

which completes the proof of Lemma 8. ∎

LEMMA 9. *For a natural number t we have*

$$\alpha_p(t, L) \leq 2^{\delta_{2,p}}(1-p^{2-m})^{-1}\max d_p(b, L)\,,$$

where b runs over non-zero integers, d_p denotes the primitive local density and δ is the Kronecker's delta function.

Proof. It is known [7], [2] that for $a \not\equiv 0 \bmod p$ and $r \geq 0$,

$$\begin{aligned}\alpha_p(ap^r, L) &= 2^{\delta_{2,p}}\sum_{0\leq k\leq r/2} p^{k(2-m)}d_p(ap^{r-2k}, L)\\ &< 2^{\delta_{2,p}}\{\max_b d_p(b, L)\}\sum_{k\geq 0} p^{k(2-m)}\\ &= 2^{\delta_{2,p}}(1-p^{2-m})^{-1}\max d_p(b, L)\,.\end{aligned}$$ ∎

LEMMA 10. *For a natural number t we have*

$$\prod_p \alpha_p(t, L) \ll (tdL)^{\varepsilon}\prod_{p\mid 2dL}\{\max_{0\neq b\in Z} d_p(b, L)\}$$

for any positive number ε.

Proof. By virtue of Lemmas 8, 9, we have

$$\begin{aligned}\prod_p \alpha_p(t, L) &\ll (tdL)^{\varepsilon}\prod_{p\mid 2dL}(1-p^{2-m})^{-1}\prod_{p\mid 2dL}\{\max_b d_p(b, L)\}\\ &\ll t^{\varepsilon}(dL)^{2\varepsilon}\prod_{p\mid 2dL}\{\max d_p(b, L)\}\,.\end{aligned}$$ ∎

LEMMA 11. *For a natural number t we have*

$$\prod_p \alpha_p(t, L) \ll (tdL)^{\varepsilon}\prod_{p\mid 2dL}\sqrt{p^{a_p}}$$

where ε is any positive number and a_p is the integer defined in Theorem.

Proof. We have only to prove

$$d_p(b, L) < C_{\varepsilon}p^{\varepsilon\,\mathrm{ord}_p dL + a_p/2}\,,$$

where C_ε depends only on ε, since $\prod_{p\mid 2dL} C_\varepsilon \ll (dL)^{\varepsilon}$. Let h be an integer such that $p^h n(L^\sharp) \subset 2pZ_p$. It is known [2]

$$d_p(b, L) = p^{\mathrm{ord}_p dL + h(1-m)}\,\sharp D(b, L; p^h)\,,$$

where

$$D(b, L; p^h) = \{x \in Z_pL/p^hZ_pL^\# \mid Q(x) \equiv b \bmod 2p^hZ_p,\ x \notin pZ_p\}.$$

Let an orthogonal splitting of Z_pL be $L_1 \perp \cdots \perp L_s$ where L_i is p^{a_i}-modular for $i \geq 2$ and $a_2 \leq \cdots \leq a_s$ and a Jordan splitting of $L_1 \perp L_2$ gives a Jordan splitting of Z_pL; then we can put $h = a_s + 2 = O(p^{\varepsilon \operatorname{ord}_p dL})$, and we have

$$\begin{aligned}
&\# D(b, L; p^h) \\
&\leq \sum_{\substack{x \in \perp L_i/p^{h-a_i} L_i \\ i \geq 2}} \#\{y \in L_1/p^hL_1^\# \mid Q(y) \equiv b - Q(x) \bmod 2p^hZ_p\} \\
&\leq p^{\sum_{i\geq 2}(h-a_i)\operatorname{rk} L_i} \max_{c \in Z} \#\{y \in L_1/p^hL_1^\# \mid Q(y) \equiv c \bmod 2p^hZ_p\}
\end{aligned}$$

and hence we have

$$d_p(b, L) \leq p^{\operatorname{ord}_p dL_1 + h(1-\operatorname{rk} L_1)} \max_{c \in Z} \#\{y \in L_1/p^hL_1^\# \mid Q(y) \equiv c \bmod 2p^hZ_p\}.$$

Suppose $Z_pL = \langle 2\varepsilon_1\rangle \perp \langle 2p^a\varepsilon_2\rangle \perp \cdots$, $\varepsilon_1, \varepsilon_2 \in Z_a^\times$, $a \geq 0$ (Jordan splitting). We put $L_1 = \langle 2\varepsilon_1\rangle \perp \langle 2p^a\varepsilon_2\rangle$; then we have

$$\begin{aligned}
&\#\{y \in L_1/p^hL_1^\# \mid Q(y) \equiv c \bmod 2p^hZ_p\} \\
&= \#\{u \bmod p^{h-\delta},\ v \bmod p^{h-a-\delta} \mid 2\varepsilon_1u^2 + 2p^a\varepsilon_2v^2 \equiv c \bmod 2p^hZ_p\},
\end{aligned}$$

where $\delta = \delta_{2,p}$

$$= O(hp^{h-a/2}) \text{ by Lemma 3. Thus we have}$$

$$d_p(b, L) \ll p^{a-h}\cdot hp^{h-a/2} < hp^{a/2} \ll p^{\varepsilon \operatorname{ord}_p dL + a/2}.$$

Next we suppose that $p = 2$ and $Z_2L = \langle 2\varepsilon\rangle \perp \left\langle 2^a\begin{pmatrix} 2d & 1 \\ 1 & 2d\end{pmatrix}\right\rangle \perp \cdots$, $\varepsilon \in Z_p^\times$, $a \geq 2$, $d = 0, 1$. Putting $L_1 = \langle 2\varepsilon\rangle \perp \left\langle 2^a\begin{pmatrix} 2d & 1 \\ 1 & 2d\end{pmatrix}\right\rangle$, we have

$$\begin{aligned}
&\#\{y \in L_1/p^hL_1^\# \mid Q(y) \equiv c \bmod 2^{h+1}Z_2\} \\
&= \#\{u \bmod 2^{h-1},\ v, w \bmod 2^{h-a} \mid 2\varepsilon u^2 + 2^{a+1}(dv^2 + vw + dw^2) \equiv c \bmod 2^{h+1}\} \\
&\ll h\cdot 2^{2h-3a/2} \qquad \text{(by Lemmas 6, 7)}.
\end{aligned}$$

Hence we have $d_2(b, L) \ll 2^{1+2a-2h}\cdot h\cdot 2^{2h-3a/2} \ll 2^{a/2+\varepsilon \operatorname{ord}_2 dL}$ as above.

Lastly we suppose $p = 2$ and $Z_2L = \left\langle\begin{pmatrix} 2d & 1 \\ 1 & 2d\end{pmatrix}\right\rangle \perp \cdots$, $d = 0$ or 1 by which we exhaust all types of Jordan splittings. Putting $L_1 = \left\langle\begin{pmatrix} 2d & 1 \\ 1 & 2d\end{pmatrix}\right\rangle$, we have

$$\begin{aligned}
&\#\{y \in L_1/2^hL_1^\# \mid Q(y) \equiv c \bmod 2^{h+1}Z_2\} \\
&= \#\{u, v \bmod 2^h \mid 2(du^2 + uv + dv^2) \equiv c \bmod 2^{h+1}\} \\
&\ll h\cdot 2^h \qquad \text{(by Lemmas 4, 5)}.
\end{aligned}$$

Therefore we have $d_2(b, L) \ll 2^{-h} \cdot h \cdot 2^h \ll 2^{\varepsilon \operatorname{ord}_2 dL}$, and it completes the proof of Lemma. ∎

Now we can prove Theorem, following an idea due to Conway, Thompson on p. 46 in [7]. Put

$$w(M) = \{\sum_{N \in \operatorname{gen} L} (\sharp O(N))^{-1}\}^{-1} \cdot (\sharp O(M))^{-1}$$

and

$$r(t, \operatorname{gen} L) = \sum_{N \in \operatorname{gen} L} w(N) r(t, N)$$

where N's run over representatives of isometry classes in the genus of L and $O(N)$ is the group of isometries of N and $r(t, N) = \sharp\{x \in N \mid Q(x) = t\}$. It is known [9] that $r(t, \operatorname{gen} L) = c(dL)^{-1/2} t^{m/2-1} \prod_p \alpha_p(t, L)$ for some constant c and hence we have

$$\sum_{t=1}^{k} r(t, \operatorname{gen} L) \ll (dL)^{-1/2} \sum_{t=1}^{k} t^{m/2-1} (tdL)^{\varepsilon} \prod_{p \mid 2dL} \sqrt{p^{a_p}} \qquad \text{(by Lemma 11)}$$
$$\ll (dL)^{\varepsilon - 1/2} \prod_{p \mid 2dL} \sqrt{p^{a_p}} \cdot k^{m/2+\varepsilon} .$$

Suppose $\sum_{x=1}^{k} r(t, M) > 0$ for every M in $\operatorname{gen} L$; then we have

$$\sum_{t=1}^{k} r(t, \operatorname{gen} L) = \sum_{M \in \operatorname{gen} L} w(M) \sum_{t=1}^{k} r(t, M) \geq \sum_{M \in \operatorname{gen} L} w(M) = 1 ,$$

and hence $k^{m/2+\varepsilon} \gg (dL)^{1/2-\varepsilon} \prod_{p \mid 2dL} \sqrt{p^{-a_p}}$. Therefore $k = C_\varepsilon (dL)^{(1/2-\varepsilon)/(m/2+\varepsilon)} \cdot (\prod_{p \mid 2dL} p^{-a_p})^{1/(m+2\varepsilon)}$ for some C_ε is contradictory for any positive number ε. Thus $\sum_{t=1}^{k} r(t, M) = 0$ holds for some $M \in \operatorname{gen} L$ and the above k and this yields $\min M > k$. Since $(1/2 - \varepsilon)/(m/2 + \varepsilon)$ tends to $1/m$ from below as $\varepsilon \to 0$ and $-(m + 2\varepsilon)^{-1} > -m^{-1}$, this means

$$\min M \gg (dL)^{1/m - \varepsilon} (\prod_{p \mid 2dL} p^{a_p})^{-1/m} \qquad \text{for any } \varepsilon > 0$$

and completes the proof of Theorem. ∎

References

[1] J. S. Hsia, Y. Kitaoka, M. Kneser, Representations of positive definite quadratic forms, J. reine angew. Math., **301** (1978), 132–141.
[2] Y. Kitaoka, Modular forms of degree n and representation by quadratic forms II, Nagoya Math. J., **87** (1982), 127–146.
[3] ——, Lectures on Siegel modular forms and representation by quadratic forms, Tata Institute of Fundamental Research, Bombay, Berlin-Heidelberg-New York, Springer 1986.

https://doi.org/10.1017/S0027763000001501 Published online by Cambridge University Press

[4] ——, Local densities of quadratic forms, In: Investigations in Number Theory, 1987 (Advanced Studies in Pure Math. 13, pp. 433–460).

[5] ——, A note on representation for positive definite binary quadratic forms by positive definite quadratic forms in 6 variables, to appear,

[6] ——, Modular forms of degree n and representation by quadratic forms V, Nagoya Math. J., **111** (1988), 173–179.

[7] J. Milnor, D. Husemoller, Symmetric bilinear forms, Berlin-Heidelberg-New York, Springer 1973.

[8] O. T. O'Meara, Introduction to quadratic forms, Berlin-Heidelberg-New York, Springer 1963.

[9] C. L. Siegel, Über die analytische Theorie der quadratischen Formen, Ann. of Math., **36** (1935), 527–606.

Department of Mathematics
School of Science
Nagoya University
Chikusa-ku, Nagoya 464
Japan

https://doi.org/10.1017/S0027763000001501 Published online by Cambridge University Press