Y. Kitaoka
Nagoya Math. J.
Vol. 107 (1987), 25-47

# MODULAR FORMS OF DEGREE $n$ AND REPRESENTATION BY QUADRATIC FORMS IV

YOSHIYUKI KITAOKA

Let $M$ be a quadratic lattice with positive definite quadratic form over the ring of rational integers, $M'$ a submodule of finite index, $S$ a finite set of primes containing all prime divisors of $2[M: M']$ and such that $M_p$ is unimodular for $p \notin S$. In [2] we showed that there is a constant $c$ such that for every lattice $N$ with positive definite quadratic form and every collection $(f_p)_{p\in S}$ of isometries $f_p$: $N_p \to M_p$ there is an isometry $f$: $N \to M$ satisfying

$$f \equiv f_p \bmod M_p' \text{ for every } p \mid [M: M'],$$
$$f(N_p) \text{ is primitive in } M_p \text{ for every } p \notin S,$$

provided the minimum of $N \geqq c$ and $\operatorname{rank} M \geqq 3 \operatorname{rank} N + 3$.

Our aim is to show that the condition $\operatorname{rank} M \geqq 3 \operatorname{rank} N + 3$ can be weakened to $\operatorname{rank} M \geqq 2 \operatorname{rank} N + 3$ if $\operatorname{rank} N = 2$. The argument suggests that it is the case without limit on rank $N$.

In Section 1 we complete a result of van der Blij [8], in Section 2 we take out the Eisenstein series from the generating theta series, in Section 3 we give an estimate of local densities from below and in Section 4 we give an asymptotic formula for numbers of isometries and show the existence of an isometry in question.

NOTATION. 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. If $A$ is a commutative ring, $M_{m,n}(A)$ is the set of $m \times n$ matrices with entries in $A$. For $X \in M_{m,n}(A)$ ${}^tX$ means the transposed matrix and we put $Y[X] = {}^tXYX$ for $Y \in M_{m,m}(A)$. $1_m$ is the unit matrix of order $m$. Let $M$ be a module over $A$ and $N$ a submodule. $N$ is called primitive if $M/N$ is a free module. Similarly $P \in M_{m,n}(A)$ $(m \geqq n)$ is called primitive

Received January 14, 1986.

if it can be completed to a matrix in $M_{m,m}(A)$ whose determinant is a unit in $A$. For a quadratic module we denote by $B(\ ,\ )$, $Q(\ )$ the associated bilinear form, quadratic form with $Q(x) = B(x, x)$ respectively.

## § 1.

Let $S \in M_{m,m}(Z)$, $T \in M_{n,n}(Z)$ $(m \geqq n)$ be symmetric positive definite matrices respectively, $P \in M_{m,n}(Z)$ and $\nu$ a natural number. They are fixed once and for all in this section. By $\mathfrak{P}\mathfrak{G}(S, \nu)$ we denote a set of all positive definite matrices $S'$ in $M_{m,m}(Z)$ such that $S' = S[U_p]$ for some $U_p \in GL_m(Z_p)$ with $U_p \equiv 1_m \bmod \nu Z_p$ for every prime $p$. If for $S', S'' \in \mathfrak{P}\mathfrak{G}(S, \nu)$ there is a unimodular matrix $U \in GL_m(Z)$ such that $S' = S''[U]$, $U \equiv 1_m \bmod \nu$, then we say that $S'$ and $S''$ are equivalent and write $S' \underset{\nu}{\sim} S''$. Put

$$\begin{aligned}
&A(S, T; P, \nu) = \sharp\{X \in M_{m,n}(Z) \mid S[X] = T, X \equiv P \bmod \nu\}, \\
&E(S, \nu) = A(S, S; 1_m, \nu), \\
&M(S, \nu) = \sum_{\mathfrak{P}\mathfrak{G}(S,\nu)/\underset{\nu}{\sim} \ni S'} 1/E(S', \nu), \\
&A_0(S, T; P, \nu) = M(S, \nu)^{-1} \sum_{\mathfrak{P}\mathfrak{G}(S,\nu)/\underset{\nu}{\sim} \ni S'} A(S', T; P, \nu)/E(S', \nu), \\
&\alpha_p(S, T; P, \nu) = 2^{-\delta_{m,n}} \lim_{a\to\infty} (p^a)^{n(n+1)2-mn} \\
&\quad \times \sharp\{X \in M_{m,n}(Z_p/p^a Z_p) \mid S[X] \equiv T \bmod p^a Z_p, X \equiv P \bmod \nu Z_p\}.
\end{aligned}$$

Here $S'$ runs over a complete set of representatives of equivalence classes in $\mathfrak{P}\mathfrak{G}(S, \nu)$ and $\delta_{m,n}$ is the Kronecker's delta function.

The purpose of this section is to prove the following theorem which is already proved in [8] if $P$ is primitive as an element in $M_{m,n}(Z_p)$ for $p \mid \nu$.

THEOREM.

$$A_0(S, T; P, \nu) = \varepsilon \delta_{\nu,m,n} \gamma_{m,n} |S|^{-n/2} |T|^{(m-n-1)/2} \prod_p \alpha_p(S, T; P, \nu),$$

*where*

$$\varepsilon = \begin{cases} 1 & \text{if } m > n+1 \text{ or } m = n = 1, \\ 1/2 & \text{otherwise,} \end{cases}$$

$$\gamma_{m,n} = \pi^{n(2m-n+1)/4} \prod_{k=0}^{n-1} \Gamma((m-k)/2)^{-1},$$

$$\delta_{\nu,m,n} = \begin{cases} 1 & \text{if } m \neq n \text{ or if } \nu = 1, 2, \\ 2^{\omega(\nu)-2} & \text{if } m = n \text{ and if } \nu \geqq 3 \text{ and } (\nu, 4) = 2, \\ 2^{\omega(\nu)-1} & \text{otherwise.} \end{cases}$$

*Here $\omega(\nu)$ denotes the number of different prime factors of $\nu$.*

The proof is proceeded along the original idea of Siegel [7].

Since Theorem is proved for $\nu = 1$, we may assume $\nu > 1$ and we fix, once and for all a natural number $\nu_0$ of a power of $\nu$ such that $\nu_0$ is divided by $|T|\nu^2$ in $Z_p$ for $p|\nu$. Then $\nu_0 \geqq 4$ holds. Put

$$G_m(r) = \{G \in GL_m(Z) | G \equiv 1_m \bmod r\}$$

for a natural number $r$ and then it is known that $G_m(r)$ is torsion-free for $r \geqq 3$.

LEMMA 1. *For $S' \in \mathfrak{PS}(S, \nu)$ we have*

$$E(S', \nu)\sharp(\{H \in \mathfrak{PS}(S, \nu) | H \underset{\nu}{\sim} S'\}/\underset{\nu_0}{\sim}) = [G_m(\nu) \colon G_m(\nu_0)] .$$

*Proof.* Considering the mapping $S' \mapsto S'[U]$ $(U \in G_m(\nu))$, we have

$$\sharp(\{H \in \mathfrak{PS}(S, \nu) | H \underset{\nu}{\sim} S'\}/\underset{\nu_0}{\sim}) = \sharp(O(S') \cap G_m(\nu) \backslash G_m(\nu)/G_m(\nu_0)) ,$$

where $O(S')$ is $\{X \in GL_m(Z) | S'[X] = S'\}$ as usual. For $U \in G_m(\nu)$ the number of $G_m(\nu_0)$ cosets in the double coset $(O(S') \cap G_m(\nu))UG_m(\nu_0)$ is equal to $\sharp(O(S') \cap G_m(\nu)/\{V \in O(S') \cap G_m(\nu) | VUG_m(\nu_0) = UG_m(\nu_0)\}) = \sharp(O(S') \cap G_m(\nu)) = E(S', \nu)$, noting that $VUG_m(\nu_0) = UG_m(\nu_0)$ implies $V \in G_m(\nu_0)$ and hence $V = 1_m$ since $V$ is of finite order and $\nu_0 \geqq 3$. This completes the proof.

LEMMA 2. *For $S' \in \mathfrak{PS}(S, \nu)$, we have*

$$A(S', T; P, \nu)/E(S', \nu) = [G_m(\nu) \colon G_m(\nu_0)]^{-1} \sum A(H, T; P, \nu)$$

*where $H$ runs over a complete set of equivalence classes*

$$\{H \in \mathfrak{PS}(S, \nu) | H \underset{\nu}{\sim} S'\}/\underset{\nu_0}{\sim} .$$

*Proof.* For $H = S'[U]$, $U \in G_m(\nu)$, we have

$$\begin{aligned} A(H, T; P, \nu) &= \sharp\{X \in M_{m,n}(Z) | H[X] = T, X \equiv P \bmod \nu\} \\ &= \sharp\{X \in M_{m,n}(Z) | S'[UX] = T, UX \equiv P \bmod \nu\} \\ &= A(S', T; P, \nu) . \end{aligned}$$

Hence Lemma 2 follows from Lemma 1.

Let $\{P_j\}$ be a complete set of representatives of $\{P' \in M_{m,n}(Z) | P' \equiv P \bmod \nu\} \bmod \nu_0$; then $P_j$ can be chosen so that $\operatorname{rank} P_j = n$ and $P_j = U_j\begin{pmatrix} B_j & A_j \\ & 0 \end{pmatrix}$ where $U_j \in GL_m(Z)$, $A_j, B_j \in M_{n,n}(Z)$ satisfies

$$(|B_j|, \nu) = 1 \quad \text{and} \quad \nu_0 A_j^{-1} \in M_{n,n}(Z) .$$

We fix such $P_j$, $A_j$ once and for all hereafter.

LEMMA 3. *Put* $Q = P_j$, $A = A_j$. *Then we have for* $S' \in \mathfrak{P}\mathfrak{G}(S, \nu)$

$$A(S', T; Q, \nu_0) = \sum_{G \in M_{m,n}(Z)/M_{m,n}(Z)A} A(S', T[A^{-1}]; (Q + \nu_0 G)A^{-1}, \nu_0)\,.$$

*Proof.* Suppose $S'[X] = T$, $X \equiv Q \mod \nu_0$ for $X \in M_{m,n}(Z)$. For $F = \nu_0^{-1}(X - Q) \in M_{m,n}(Z)$ we have $S'[XA^{-1}] = T[A^{-1}]$ and

$$XA^{-1} = QA^{-1} + \nu_0 FA^{-1} \in M_{m,n}(Z)\,.$$

If, conversely $S'[Y] = T[A^{-1}]$, $Y \equiv (Q + \nu_0 G)A^{-1} \mod \nu_0$, then $S'[YA] = T$ and $YA \equiv Q \mod \nu_0$ hold.

LEMMA 4. *Let* $P_j$, $A_j$ *be those as above. Then we have*

$$\begin{aligned} A_0(S, T; P, \nu) = {} & M(S, \nu_0)M(S, \nu)^{-1}[G_m(\nu): G_m(\nu_0)]^{-1}\varepsilon\delta_{\nu,m,n}\gamma_{m,n} \\ & \times |S|^{-n/2}|T|^{(m-n-1)/2} \prod_{p \nmid \nu} \alpha_p(S, T; P, \nu) \\ & \times \sum_{S_i} \{\sum_{P_j} \sum_{G \in M_{m,n}(Z)/M_{m,n}(Z)A_j} \|A_j\|^{n+1-m} \\ & \times \prod_{p|\nu} \alpha_p(S_i, T[A_j^{-1}]; (P_j + \nu_0 G)A_j^{-1}, \nu_0)\}\,, \end{aligned}$$

*where* $P_j$ *runs over a complete set of representatives of* $\{P' \in M_{m,n}(Z) | P' \equiv P \mod \nu\} \mod \nu_0$ *given above and* $\{S_i\}$ *is given so that* $\mathfrak{P}\mathfrak{G}(S, \nu) = \coprod_i \mathfrak{P}\mathfrak{G}(S_i, \nu_0)$ *(disjoint union).*

*Proof.* By definition we have

$$\begin{aligned} A_0(S, T; P, \nu) &= M(S, \nu)^{-1} \sum_{\mathfrak{P}\mathfrak{G}(S,\nu)/\underset{\nu}{\sim} \ni S'} A(S', T; P, \nu)/E(S', \nu) \\ &= M(S, \nu)^{-1}[G_m(\nu): G_m(\nu_0)]^{-1} \sum_{\mathfrak{P}\mathfrak{G}(S,\nu)/\underset{\nu}{\sim} \ni S'} \sum A(H, T; P, \nu)\,, \end{aligned}$$

by Lemma 2, where $H$ runs over $\{H \in \mathfrak{P}\mathfrak{G}(S, \nu) | H \underset{\nu}{\sim} S'\}/\underset{\nu_0}{\sim}$

$$\begin{aligned} &= M(S, \nu)^{-1}[G_m(\nu): G_m(\nu_0)]^{-1} \sum_{\mathfrak{P}\mathfrak{G}(S,\nu)/\underset{\nu_0}{\sim} \ni H} A(H, T; P, \nu) \\ &= M(S, \nu)^{-1}[G_m(\nu): G_m(\nu_0)]^{-1} \sum_{S_i} \sum_{\mathfrak{P}\mathfrak{G}(S_i,\nu_0)/\underset{\nu_0}{\sim} \ni H} A(H, T; P, \nu) \\ &= M(S, \nu)^{-1}[G_m(\nu): G_m(\nu_0)]^{-1} \sum_{P_j, S_i} \sum_{\mathfrak{P}\mathfrak{G}(S_i,\nu_0)/\underset{\nu_0}{\sim} \ni H} A(H, T; P_j, \nu_0) \\ &= M(S, \nu)^{-1}[G_m(\nu): G_m(\nu_0)]^{-1} \sum_{P_j, S_i} \sum_{\mathfrak{P}\mathfrak{G}(S_i,\nu_0)/\underset{\nu_0}{\sim} \ni H} \\ &\quad \times \sum_{G \in M_{m,m}(Z)/M_{m,n}(Z)A_j} A(H, T[A_j^{-1}]; (P_j + \nu_0 G)A_j^{-1}, \nu_0)\,, \end{aligned}$$

by Lemma 3.

For $H \in \mathfrak{P}\mathfrak{G}(S, \nu)$ we have $M(H, \nu_0)^{-1} = A_0(H, H; 1_m, \nu_0) = A_0(S, S; 1_m, \nu_0)$

$= M(S, \nu_0)^{-1}$, noting that the definition implies the first and third equality and the second follows from $\alpha_p(H, H; 1_m, \nu_0) = \alpha_p(S, S; 1_m, \nu_0)$ in the proved case. If $T[A_j^{-1}]$ is integral, then $|A_j|^2$ divides $|T|$ and hence $\nu_0/\nu$ is divided by $|A_j|$; then $(P_j + \nu_0 G)A_j^{-1} \equiv P_j A_j^{-1} \bmod \nu$. By virtue of definition of $A_j$, $P_j A_j^{-1} \in M_{m,n}(Z_p)$ is primitive for $p|\nu$ and hence $(P_j + \nu_0 G)A_j^{-1}$ is also primitive for $p|\nu$. Using Theorem which is proved for a primitive $P$ for $p|\nu$, we have

$$\begin{aligned} A_0(S, T; P, \nu) &= M(S, \nu_0)M(S, \nu)^{-1}[G_m(\nu): G_m(\nu_0)]^{-1}\varepsilon\delta_{\nu,m,n}\gamma_{m,n}|S|^{-n/2} \\ &\times |T|^{(m-n-1)/2} \prod_{p\nmid\nu} \alpha_p(S, T; P, \nu)\{\sum_{P_j, S_i} \sum_{G \in M_{m,n}(Z)/M_{m,n}(Z)A_j} \|A_j\|^{n+1-m} \\ &\times \prod_{p|\nu} \alpha_p(S, T[A_j^{-1}]; (P_j + \nu_0 G)A_j^{-1}, \nu_0)\}, \end{aligned}$$

since for $p \nmid \nu$ $\alpha_p(S, T[A_j^{-1}]; (P_j + \nu_0 G)A_j^{-1}, \nu_0) = \alpha_p(S, T) = \alpha_p(S, T; P, \nu)$.

Let $q$ be a sufficiently large power of $\nu_0$ and put $\Lambda = \{F \in M_{n,n}(Z) | F = {}^tF\}$.

LEMMA 5. *Put* $Q = P_j$, $A = A_j$ *and denote by* $\mathscr{R}$ $\{qR[A^{-1}] | R \in \Lambda\}$. *Then the mapping* $Y \mapsto YA$ *is bijective from*

$$\coprod_{R \in \mathscr{R}/q\Lambda} \left\{ Y \in M_{m,n}(Z/qZ) \,\middle|\, \begin{array}{l} S[Y] \equiv T[A^{-1}] + R \bmod q, \\ Y \equiv (Q + \nu_0 G)A^{-1} \bmod \nu_0 \\ \textit{for some } G \in M_{m,n}(Z) \end{array} \right\}$$

*to*

$$\{X \in M_{m,n}(Z) \bmod qM_{m,n}(Z)A \,|\, S[X] \equiv T \bmod q,\ X \equiv Q \bmod \nu_0\}.$$

*Proof.* The mapping is clearly well-defined and injective. Suppose, conversely that $X \in M_{m,n}(Z)$ satisfies $S[X] \equiv T \bmod q$ and $X \equiv Q \bmod \nu_0$. Defining $G \in M_{m,n}(Z)$ by $X = Q + \nu_0 G$, $XA^{-1} = QA^{-1} + \nu_0 GA^{-1}$ is integral. For $R = q^{-1}(S[X] - T) \in M_{n,n}(Z)$ and $Y = XA^{-1}$ we have $S[Y] = T[A^{-1}] + qR[A^{-1}]$. This shows the surjectiveness of the mapping.

LEMMA 6. *Let* $V, W$ *be regular quadratic spaces over* $\boldsymbol{Q}_p$ *and* $M, N$ *lattices on* $V, W$ *respectively* ($\dim V = \operatorname{rank} M$, $\dim W = \operatorname{rank} N$). *Let* $h$ *be an integer such that*

$$p^h Q(x) \in 2Z_p \qquad \textit{for all } x \in M^{\#},$$

*where* $M^{\#} = \{x \in V | B(x, M) \subset Z_p\}$. *If* $u \in \operatorname{Hom}(M, N)$ *satisfies*

$$Q(x) \equiv Q(u(x)) \bmod 2p^{h+1}Z_p \qquad \textit{for } x \in M,$$

*then there is an isometry* $u'$ *from* $M$ *to* $N$ *such that*

$$u'(M) = u(M)\,,$$
$$u'(x) \equiv u(x) \bmod p^{h+1}u(M^\sharp) \qquad \textit{for } x \in M\,.$$

Especially we have $u' : M \cong u(M)$.

*Proof.* Since for $y, z \in M^\sharp$ $2B(y, z) = Q(y+z) - Q(y) - Q(z) \in 2p^{-h}\boldsymbol{Z}_p$ holds, we have $B(p^h y, z) \in \boldsymbol{Z}_p$ and hence $p^h M^\sharp \subset (M^\sharp)^\sharp = M$. Next we claim that for $G = u(M^\sharp)$ the three conditions

$$\begin{aligned} &\mathrm{Hom}\,(M, \boldsymbol{Z}_p) = \{x \mapsto B(u(x), w) \,|\, w \in G\} + \mathrm{Hom}\,(M, p\boldsymbol{Z}_p)\,, \\ &p^h Q(x) \in 2\boldsymbol{Z}_p \qquad \text{for } x \in G, \\ &Q(u(x)) \equiv Q(x) \bmod 2p^{h+1}\boldsymbol{Z}_p \qquad \text{for } x \in M \end{aligned}$$

are satisfied. Let $\varphi$ be an element of $\mathrm{Hom}\,(M, \boldsymbol{Z}_p)$; then there is $z \in M^\sharp$ such that $\varphi(x) = B(x, z)$ for $x \in M$. For $x \in M$ we have

$$p^h\varphi(x) = B(x, p^h z) \equiv B(u(x), p^h u(z)) \bmod p^{h+1}\boldsymbol{Z}_p\,,$$

since $p^h z \in M$. Thus $x \mapsto \varphi(x) - B(u(x), u(z))$ is in $\mathrm{Hom}\,(M, p\boldsymbol{Z}_p)$ and the first condition holds. For $x \in M^\sharp$ we have

$$Q(p^h x) \equiv Q(p^h u(x)) \bmod 2p^{h+1}\boldsymbol{Z}_p$$

and then $p^h Q(x) \equiv p^h Q(u(x)) \bmod 2p\boldsymbol{Z}_p$. From the assumption $p^h Q(x) \in 2\boldsymbol{Z}_p$ holds and hence $p^h Q(u(x)) \in 2\boldsymbol{Z}_p$ holds. Thus the second condition holds. The third one is nothing but the assumption. "Satz" in Section 14 in [5] completes the proof.

LEMMA 7. *For $Q = P_j$ and $A = A_j$ we have*

$$\begin{aligned} &\sharp\{X \bmod q \,|\, S[X] \equiv T \bmod q,\ X \equiv Q \bmod \nu_0\} \\ &\quad = \|A\|^{n+1-m} \sum_{G \in M_{m,n}(\boldsymbol{Z})/M_{m,n}(\boldsymbol{Z})A} \sharp\left\{ Y \bmod q \,\middle|\, \begin{array}{l} S[Y] \equiv T[A^{-1}] \bmod q \\ Y \equiv (Q + \nu_0 G)A^{-1} \bmod \nu_0 \end{array} \right\}. \end{aligned}$$

*Proof.* By Lemma 5 we have

$$\begin{aligned} &\sharp\{X \bmod q \,|\, S[X] \equiv T \bmod q,\ X \equiv Q \bmod \nu_0\} \\ &\quad = \|A\|^{-m}\sharp\{X \in M_{m,n}(\boldsymbol{Z})/qM_{m,n}(\boldsymbol{Z})A \,|\, S[X] \equiv T \bmod q,\ X \equiv Q \bmod \nu_0\} \\ &\quad = \|A\|^{-m} \sum_{R \in \mathscr{R}/qA} \sharp\left\{ Y \bmod q \,\middle|\, \begin{array}{l} S[Y] \equiv T[A^{-1}] + R \bmod q \\ Y \equiv (Q + \nu_0 G)A^{-1} \bmod \nu_0 \\ \text{for some } G \in M_{m,n}(\boldsymbol{Z}) \end{array} \right\}. \end{aligned}$$

Here for a prime $p|\nu$ we define quadratic lattices $M = \boldsymbol{Z}_p[v_1, \cdots, v_n]$ and

$N = Z_p[u_1, \cdots, u_n]$ by $(B(v_i, v_j)) = T[A^{-1}]$, $(B(u_i, u_j)) = T[A^{-1}] + R$ $(R \in \mathscr{R})$ respectively. Define a linear mapping $u \in \mathrm{Hom}(M, N)$ by $u(v_i) = u_i$; then $Q(u(x)) \equiv Q(x) \bmod q\nu_0^{-2}$ holds for $x \in M$ since $R \equiv 0 \bmod q\nu_0^{-2}$. From Lemma 6 follows that there is an isometry $u'$ from $M$ to $N$ such that

$$u'(x) \equiv u(x) \bmod 2^{-1}q\nu_0^{-2}u(M^\sharp) \qquad \text{for } x \in M\,.$$

If, hence we define $D_p \in GL_n(Z_p)$ by

$$(u'(v_1), \cdots, u'(v_n)) = (u_1, \cdots, u_n)D_p\,,$$

then $T[A^{-1}] = (T[A^{-1}] + R)[D_p]$ and $D_p \equiv 1_n \bmod \nu_0 Z_p$ since $q$ is sufficiently large. Taking $D \in M_n(Z)$ which is close to $D_p$ for $p|\nu$ and considering the mapping $Y \mapsto YD$, we have

$$\begin{aligned}&\sharp\{X \bmod q \,|\, S[X] \equiv T \bmod q,\, X \equiv Q \bmod \nu_0\}\\ &\quad = \|A\|^{-m} \sum_{R \in \mathscr{R}/qA} \sharp\left\{ Y \bmod q \;\middle|\; \begin{array}{l} S[Y] \equiv T[A^{-1}] \bmod q \\ Y \equiv (Q + \nu_0 G)A^{-1} \bmod \nu_0 \\ \text{for some } G \in M_{m,n}(Z) \end{array} \right\}.\end{aligned}$$

Since $\sharp(\mathscr{R}/qA) = \|A\|^{n+1}$, we complete the proof.

Now we can prove the theorem. Since

$$\begin{aligned}&\sharp\{X \bmod q \,|\, S[X] \equiv T \bmod q,\, X \equiv P \bmod \nu\}\\ &\quad = \sum_{P_j} \sharp\{X \bmod q \,|\, S[X] \equiv T \bmod q,\, X \equiv P_j \bmod \nu_0\}\,,\end{aligned}$$

Lemma 7 implies

$$\begin{aligned}&\prod_{p|\nu} \alpha_p(S, T; P, \nu)\\ &\quad = \sum_{P_j} \sum_{G \in M_{m,n}(Z)/M_{m,n}(Z)A_j} \|A_j\|^{n+1-m} \prod_{p|\nu} \alpha_p(S, T[A_j^{-1}]; (P_j + \nu_0 G)A_j^{-1}, \nu_0)\end{aligned}$$

and then from Lemma 4 follows

$$\begin{aligned}A_0(S, T; P, \nu) &= M(S, \nu_0)M(S, \nu)^{-1}[G_m(\nu)\colon G_m(\nu_0)]^{-1}\varepsilon\delta_{\nu,m,n}\gamma_{m,n}\\ &\quad \times |S|^{-n/2}|T|^{(m-n-1)/2} \sum_{S_i} \prod_p \alpha_p(S_i, T; P, \nu)\,.\end{aligned}$$

Since $S_i \in \mathfrak{P}\mathfrak{G}(S, \nu)$ implies $\alpha_p(S_i, T; P, \nu) = \alpha_p(S, T; P, \nu)$, we have

$$A_0(S, T; P, \nu) = c\varepsilon\delta_{\nu,m,n}\gamma_{m,n}|S|^{-n/2}|T|^{(m-n-1)/2} \prod_p \alpha_p(S, T; P, \nu)$$

where $c = M(S, \nu_0)M(S, \nu)^{-1}[G_m(\nu)\colon G_m(\nu_0)]^{-1}\sharp\{S_i\}$. Hence $c$ depends only on $S$ for a sufficiently large power of $\nu$. Since Theorem holds for $c = 1$ in case $T = S$, we have $c = 1$ and complete the proof of Theorem.

https://doi.org/10.1017/S002776300000252X Published online by Cambridge University Press

## § 2.

Let $S \in M_{m,m}(\boldsymbol{Z})$ be a symmetric positive definite matrix whose diagonals are even integers and $q$ the level of $S$, that is, $qS^{-1}$ is also integral and diagonal entries of $qS^{-1}$ are even.

Let $P$ be an element of $M_{m,n}(\boldsymbol{Z})$ and $\nu$ a natural number. For $Z = {}^tZ \in M_n(\boldsymbol{C})$ with $\operatorname{Im} Z > 0$, we put

$$\theta(Z, S, P, \nu) = \sum_{N \equiv -P \bmod \nu} \exp(\pi i \operatorname{tr}(Z \cdot S[N])),$$

where $N$ runs over $\{N \in M_{m,n}(\boldsymbol{Z}) \mid N \equiv -P \bmod \nu\}$, and

$$\begin{aligned}\theta_S^{(n)}&(Z; X, Y)\\ &= \sum_{N \in M_{m,n}(\boldsymbol{Z})} \exp(\pi i \operatorname{tr}(Z \cdot S[N - Y] + 2\pi i \operatorname{tr}({}^tNX) - \pi i \operatorname{tr}({}^tXY)).\end{aligned}$$

It is easy to see $\theta(Z, S, P, \nu) = \theta_S^{(n)}(\nu^2 Z; 0, \nu^{-1}P)$, and the following lemma is nothing but Theorem 1 in [1].

LEMMA 1. *Let* $\Gamma_0^{(n)}(q) = \left\{M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in Sp_n(\boldsymbol{Z}) \mid C \equiv 0 \bmod q\right\}$. *Then for any matrix* $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ *in* $\Gamma_0^{(n)}(q)$ *the generalized theta series satisfies*

$$\begin{aligned}|CZ + D|^{-m/2}\theta_S^{(n)}(M\langle Z\rangle; X\,{}^tA + SY\,{}^tB, S^{-1}X\,{}^tC + Y\,{}^tD)\\ = \chi_S^{(n)}(M)\theta_S^{(n)}(Z; X, Y),\end{aligned}$$

*where* $\chi_S^{(n)}(M)$ *is some eighth root of unity not depending on* $X$ *or* $Y$.

For $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in Sp_n(\boldsymbol{Z})$ with $C \equiv 0 \bmod q\nu^2$, $D \equiv 1_n \bmod \nu$ we put $M' = \begin{pmatrix} A & B\nu^2 \\ C\nu^{-2} & D \end{pmatrix}$. Then we have $M' \in \Gamma_0^{(n)}(q)$ and putting $X = 0$, $Y = \nu^{-1}P$ and $Z \to \nu^2 Z$ in the lemma we have

$$\begin{aligned}|CZ + D|^{-m/2}\theta_S^{(n)}(\nu^2 M\langle Z\rangle; \nu SP\,{}^tB, \nu^{-1}P\,{}^tD)\\ = \chi_S^{(n)}(M')\theta_S^{(n)}(\nu^2 Z; 0, \nu^{-1}P)\\ = \chi_S^{(n)}(M')\theta(Z, S, P, \nu).\end{aligned}$$

Since $\nu SP\,{}^tB$ is integral and $\operatorname{tr}{}^t(\nu SP\,{}^tB)\nu^{-1}P\,{}^tD = \operatorname{tr} B\,{}^tPSP\,{}^tD = \operatorname{tr}(S[P] \cdot {}^tDB) \equiv 0 \bmod 2$, we have

$$\theta_S^{(n)}(\nu^2 M\langle Z\rangle; \nu SP\,{}^tB, \nu^{-1}P\,{}^tD) = \theta_S^{(n)}(\nu^2 M\langle Z\rangle; 0, \nu^{-1}P) = \theta(M\langle Z\rangle, S, P, \nu).$$

Thus we have proved

LEMMA 2. *For* $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in Sp_n(Z)$ *with* $M \equiv 1_{2n} \bmod q\nu^2$ *we have*

$$|CZ + D|^{-m/2}\theta(M\langle Z\rangle, S, P, \nu) = \chi(M)\theta(Z, S, P, \nu),$$

*where* $\chi(M)$ *is some eighth root of unity not depending on* $P$.

Next we prove

LEMMA 3. *Let* $S' \in \mathfrak{P}\mathfrak{S}(S, \nu)$ *in the sense of Section* 1. *Then for* $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in Sp_n(Z)$ *the constant term of the Fourier expansion of*

$$|CZ + D|^{-m/2}(\theta(M\langle Z\rangle, S, P, \nu) - \theta(M\langle Z\rangle, S', P, \nu))$$

*vanishes.*

*Proof.* For $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in Sp_n(Z)$ we put

$$\theta(Z, S, P, \nu)\Big|\begin{pmatrix} A & B \\ C & D \end{pmatrix} = |CZ + D|^{-m/2}\theta(M\langle Z\rangle, S, P, \nu).$$

First suppose $|C| \neq 0$; then noting $M\langle Z\rangle = (AZ + B)(CZ + D)^{-1} = AC^{-1} - (Z + C^{-1}D)^{-1}[C^{-1}]$, we have

$$\begin{aligned}
&\theta(Z, S, P, \nu)\Big|\begin{pmatrix} A & B \\ C & D \end{pmatrix} \\
&\quad = |CZ + D|^{-m/2}\theta_S^{(n)}(\nu^2 M\langle Z\rangle; 0, \nu^{-1}P) \\
&\quad = |CZ + D|^{-m/2}\theta_S^{(n)}(\nu^2 AC^{-1} - \nu^2(Z + C^{-1}D)^{-1}[C^{-1}]; 0, \nu^{-1}P) \\
&\quad = |CZ + D|^{-m/2}\sum_{N \in M_{m,n}(Z)} \exp(\pi i \operatorname{tr}(\nu^2 AC^{-1} - \nu^2(Z + C^{-1}D)^{-1}[C^{-1}]) \\
&\qquad \times S[N - \nu^{-1}P]).
\end{aligned}$$

Decomposing $N$ as $N = N_1 + |C|N_2$, we have

$$\operatorname{tr}(\nu^2 AC^{-1}\cdot S[N - \nu^{-1}P]) \equiv \operatorname{tr}(AC^{-1}\cdot S[\nu N_1 - P]) \bmod 2.$$

Thus $\theta(Z, S, P, \nu)\Big|\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ is equal to

$$\begin{aligned}
&|CZ + D|^{-m/2}\sum_{N_1 \bmod |C|} \exp(\pi i \operatorname{tr}(AC^{-1}\cdot S[\nu N_1 - P])) \\
&\quad \times \sum_{N_2 \in M_{m,n}(Z)} \exp(-\pi i \operatorname{tr}((Z + C^{-1}D)^{-1}[C^{-1}])\cdot S[\nu N_1 + \nu|C|N_2 - P])) \\
&= |CZ + D|^{-m/2}\sum_{N_1 \bmod |C|} \exp(\pi i \operatorname{tr}(AC^{-1}\cdot S[\nu N_1 - P]) \\
&\quad \times \theta_S^{(n)}(-\nu^2|C|^2(Z + C^{-1}D)^{-1}[C^{-1}]; 0, \nu^{-1}|C|^{-1}P - |C|^{-1}N_1) \\
&= |CZ + D|^{-m/2}\sum_{N_1 \bmod |C|} \exp(\pi i \operatorname{tr} AC^{-1}\cdot S[\nu N_1 - P])
\end{aligned}$$

https://doi.org/10.1017/S002776300000252X Published online by Cambridge University Press

$$\times |S|^{-n/2}|i\nu^2|C|^2(Z+C^{-1}D)^{-1}[C^{-1}]|^{-m/2}\theta^{(n)}_{S^{-1}}(\nu^{-2}|C|^{-2}(Z+C^{-1}D)[{}^tC];\ \nu^{-1}|C|^{-1}P-|C|^{-1}N_1, 0)$$

by Lemma 2 in [1]. Here

$$|CZ+D|^{-m/2}|i\nu^2|C|^2(Z+C^{-1}D)^{-1}[C^{-1}]|^{-m/2}$$

is a constant $\kappa(M)$ depending only on $M$. Hence the constant term of $\theta(Z, S, P, \nu)|M$ is equal to

$$\kappa(M)|S|^{-n/2}\sum_{N_1 \bmod |C|}\exp(\pi i \operatorname{tr} AC^{-1}\cdot S[\nu N_1 - P])\,.$$

Since $S' \in \mathfrak{PG}(S, \nu)$, we have $|S'| = |S|$ and there is some $U \in M_m(Z)$ such that $(|U|, \nu|C|) = 1$, $S \equiv S'[U] \bmod 2|C|$ and $U \equiv 1 \bmod \nu$. Hence it is clear that the constant term of $\theta(Z, S, P, \nu)|M$ depends only on $\mathfrak{PG}(S, \nu)$.

If the determinant of the $C$-part of $M$ vanishes, then there is an integral symmetric matrix $F$ such that $M = \begin{pmatrix} A & B \\ C & D\end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & F\end{pmatrix}$ with $|C| \neq 0$. Putting $M' = \begin{pmatrix} A & B \\ C & D\end{pmatrix}$, from the above follows

$$\begin{aligned}&\theta(Z, S, P, \nu)|M' \\ &\quad = \kappa(M')|S|^{-n/2}\sum_{N_1 \bmod |C|}\exp(\pi i \operatorname{tr} AC^{-1}\cdot S[\nu N_1 - P]) \\ &\qquad \times \theta^{(n)}_{S^{-1}}(\nu^{-2}|C|^{-2}(Z+C^{-1}D)[{}^tC];\ \nu^{-1}|C|^{-1}P-|C|^{-1}N_1, 0)\,.\end{aligned}$$

Hence we have

$$\begin{aligned}&\theta(Z, S, P, \nu)|M \\ &\quad = \kappa(M')|S|^{-n/2}\sum_{N \bmod |C|}\exp(\pi i \operatorname{tr} AC^{-1}\cdot S[\nu N - P]) \\ &\qquad \times \theta^{(n)}_{S^{-1}}(\nu^{-2}|C|^{-2}(Z+C^{-1}D)[{}^tC];\ \nu^{-1}|C|^{-1}P-|C|^{-1}N, 0)\Big|\begin{pmatrix} 0 & 1 \\ -1 & F\end{pmatrix}.\end{aligned}$$

Here we don't care for the choice of the branch of $|*|^{-m/2}$ since it is independent of $S$.

$$\theta^{(n)}_{S^{-1}}(\nu^{-2}|C|^{-2}(Z+C^{-1}D)[{}^tC];\ \nu^{-1}|C|^{-1}P-|C|^{-1}N, 0)\Big|\begin{pmatrix} 0 & 1 \\ -1 & F\end{pmatrix}$$

is equal to

$$\begin{aligned}&|-Z+F|^{-m/2}\theta^{(n)}_{S^{-1}}(\nu^{-2}|C|^{-2}((-Z+F)^{-1}+C^{-1}D)[{}^tC];\ \nu^{-1}|C|^{-1}P-|C|^{-1}N, 0) \\ &\quad = |-Z+F|^{-m/2}\sum_{G \in M_{m,n}(Z)}\exp(\pi i \operatorname{tr}(\nu^{-2}|C|^{-2}((-Z+F)^{-1}+C^{-1}D)[{}^tC] \\ &\qquad \times S^{-1}[G]) + 2\pi i \operatorname{tr}{}^tG(\nu^{-1}|C|^{-1}P-|C|^{-1}N))\,.\end{aligned}$$

Putting $G = q\nu^2|C|^2G_1 + G_2$, we have

$$\begin{aligned}
&\operatorname{tr}(\nu^{-2}|C|^{-2}((-Z+F)^{-1}+C^{-1}D)[{}^tC]\cdot S^{-1}[G] + 2\operatorname{tr}{}^tG(\nu^{-1}|C|^{-1}P - |C|^{-1}N)\\
&\quad\equiv \operatorname{tr}(\nu^{-2}|C|^{-2}(-Z+F)^{-1}[{}^tC]\cdot S^{-1}[q\nu^2|C|^2G_1+G_2]\\
&\qquad + \nu^{-2}|C|^{-2}D{}^tC\cdot S^{-1}[G_2]) + 2\operatorname{tr}{}^tG_2(\nu^{-1}|C|^{-1}P - |C|^{-1}N) \bmod 2\,.
\end{aligned}$$

Hence

$$\begin{aligned}
&\theta^{(n)}_{S^{-1}}(\nu^{-2}|C|^{-2}(Z+C^{-1}D)[{}^tC];\nu^{-1}|C|^{-1}P-|C|^{-1}N,0)\Big|\begin{pmatrix}0 & 1\\ -1 & F\end{pmatrix}\\
&= |-Z+F|^{-m/2}\sum_{G_2 \bmod q\nu^2|C|^2}\exp(\pi i\nu^{-2}|C|^{-2}\operatorname{tr}D{}^tC\cdot S^{-1}[G_2]\\
&\quad + 2\pi i\operatorname{tr}{}^tG_2(\nu^{-1}|C|^{-1}P-|C|^{-1}N))\\
&\quad \times\sum_{G_1}\exp(\pi iq^2\nu^2|C|^2\operatorname{tr}(-Z+F)^{-1}[{}^tC]S^{-1}[G_1+q^{-1}\nu^{-2}|C|^{-2}G_2])\\
&= |-Z+F|^{-m/2}\sum_{G_2 \bmod q\nu^2|C|^2}\exp(\pi i\nu^{-2}|C|^{-2}\operatorname{tr}D{}^tC\cdot S^{-1}[G_2]\\
&\quad + 2\pi i\operatorname{tr}{}^tG_2(\nu^{-1}|C|^{-1}P-|C|^{-1}N))\\
&\quad \times\theta^{(n)}_{S^{-1}}(q^2\nu^2|C|^2(-Z+F)^{-1}[{}^tC];0,-q^{-1}\nu^{-2}|C|^{-2}G_2)\\
&= |-Z+F|^{-m/2}\sum_{G \bmod q\nu^2|C|^2}\exp(\pi i\nu^{-2}|C|^{-2}\operatorname{tr}D{}^tC\cdot S^{-1}[G]\\
&\quad + 2\pi i\operatorname{tr}{}^tG(\nu^{-1}|C|^{-1}P-|C|^{-1}N))|S^{-1}|^{-n/2}\\
&\quad \times|-iq^2\nu^2|C|^2(-Z+F)^{-1}[{}^tC]|^{-m/2}\\
&\quad \times\theta^{(n)}_{S}(-q^{-2}\nu^{-2}|C|^{-2}(-Z+F)[C^{-1}];-q^{-1}\nu^{-2}|C|^{-2}G,0)\,,
\end{aligned}$$

where $|-Z+F|^{-m/2}|-iq^2\nu^2|C|^2(-Z+F)^{-1}[{}^tC]|^{-m/2}$ is independent of $Z$ and denoting it by $\kappa'(M)$

$$\begin{aligned}
&= \kappa'(M)|S|^{n/2}\sum_{G \bmod q\nu^2|C|^2}\exp(\pi i\nu^{-2}|C|^{-2}\operatorname{tr}D{}^tC\cdot S^{-1}[G]\\
&\quad + 2\pi i\operatorname{tr}{}^tG(\nu^{-1}|C|^{-1}P-|C|^{-1}N))\\
&\quad \times\theta^{(n)}_{S}(q^{-2}\nu^{-2}|C|^{-2}(Z-F)[C^{-1}];-q^{-1}\nu^{-2}|C|^{-2}G,0)\,.
\end{aligned}$$

Thus the constant term of $\theta(Z,S,P,\nu)|M$ is

$$\begin{aligned}
&\kappa(M')|S|^{-n/2}\sum_{N \bmod |C|}\exp(\pi i\operatorname{tr}AC^{-1}\cdot S[\nu N-P]\\
&\quad\times\kappa'(M)|S|^{n/2}\sum_{G \bmod q\nu^2|C|^2}\exp(\pi i\nu^{-2}|C|^{-2}\operatorname{tr}D\,{}^tC\cdot S^{-1}[G]\\
&\quad + 2\pi i\operatorname{tr}{}^tG(\nu^{-1}|C|^{-1}P-|C|^{-1}N))\\
&= \kappa(M')\kappa'(M)\sum_{\substack{N \bmod \nu|C|\\ N\equiv -P \bmod \nu\\ G \bmod q\nu^2|C|^2}}\exp(\pi i\operatorname{tr}AC^{-1}\cdot S[N]\\
&\quad + \pi i\nu^{-2}|C|^{-2}\operatorname{tr}D\,{}^tC\cdot S^{-1}[G] - 2\pi i\nu^{-1}|C|^{-1}\operatorname{tr}{}^tGN)\,.
\end{aligned}$$

Since $S' \in \mathfrak{P}\mathfrak{G}(S, \nu)$, there is some $U \in M_m(\boldsymbol{Z})$ such that

$$S \equiv S'[U] \bmod 2q\nu^2|C|^2|S|^2 ,$$
$$(|U|, 2q\nu|C||S|) = 1 ,$$
$$U \equiv 1 \bmod \nu.$$

Taking an integral matrix $V$ such that $UV \equiv 1 \bmod 2q\nu^2|C|^2|S|^2$ and multiplying integral matrices $|S|S^{-1}, |S|VS'^{-1}$ to $S \equiv {}^tUS'U \bmod 2q\nu^2|C|^2|S|^2$ from the left, the right respectively, we have

$$|S|^2VS'^{-1} \equiv |S|^2S^{-1}\,{}^tU \bmod 2q\nu^2|C|^2|S|^2$$

and hence we have

$$S^{-1} \equiv S'^{-1}[{}^tV] \bmod 2q\nu^2|C|^2 .$$

Hence the above constant term is

$$\begin{aligned}\kappa(M')\kappa'(M) &\sum_{\substack{N \bmod \nu|C| \\ N \equiv -P \bmod \nu \\ G \bmod q\nu^2|C|^2}} \exp(\pi i \operatorname{tr} AC^{-1}\cdot S'[UN] \\ &\quad + \pi i\nu^{-2}|C|^{-2} \operatorname{tr} D\,{}^tC\cdot S'^{-1}[{}^tVG] - 2\pi i\nu^{-1}|C|^{-1} \operatorname{tr} {}^t({}^tVG)(UN)) \\ = \kappa(M')\kappa'(M) &\sum_{\substack{N \bmod \nu|C| \\ N \equiv -P \bmod \nu \\ G \bmod q\nu^2|C|^2}} \exp(\pi i \operatorname{tr} AC^{-1}\cdot S'[N] \\ &\quad + \pi i\nu^{-2}|C|^{-2} \operatorname{tr} D\,{}^tC\cdot S'^{-1}[G] - 2\pi i\nu^{-1}|C|^{-1} \operatorname{tr} {}^tGN) .\end{aligned}$$

Thus we have proved Lemma 3.

Put $E(Z, S, P, \nu) = M(S, \nu)^{-1} \sum_{S' \in \mathfrak{P}\mathfrak{G}(S,\nu)/\tilde{\nu}} E(S', \nu)^{-1}\theta(Z, S', P, \nu)$. Then $g(Z) = \theta(Z, S, P, \nu) - E(Z, S, P, \nu)$ is a Siegel modular form of level $q\nu^2$, weight $m/2$ such that the constant term of $g|M$ vanishes for every $M$ in $Sp_n(\boldsymbol{Z})$.

The Fourier coefficient of $E(Z, S, P, \nu)$ is

$$A_0(S, T; -P, \nu) \qquad \text{for } T > 0 ,$$

and for Fourier coefficients $a(T)$ of $g(Z)$ we have ([3] or [4])

$$a(T) = O((\min T)^{(3-m/2)/2}|T|^{(m-3)/2}) \qquad \text{for } T > 0$$

if $n = 2$ and $m \geqq 2n + 3$.

Clearly we have, for every integral positive definite matrix $T$

$$A(S, T; -P, \nu) = A_0(S, T; -P, \nu) + a(T) .$$

§ 3.

Let $p$ be a prime and fix an integer $a$.

Let $S \in M_{m,m}(\boldsymbol{Z}_p)$, $T \in M_{n,n}(\boldsymbol{Z}_p)$ be regular symmetric matrices with $m \geqq 2n+3$ respectively and $P \in M_{m,n}(\boldsymbol{Z}_p)$. An aim in this section is to prove

PROPOSITION. *There is a positive number $\kappa(S, P, a)$ such that $\alpha_p(S, T; P, p^a) > \kappa(S, P, a)$ if $\alpha_p(S, T; P, p^a) \neq 0$.*

We need several lemmas.

LEMMA 1. *Let $M$ be a regular quadratic lattice over $\boldsymbol{Z}_p$ with $\operatorname{rk} M = m$ and $N$ a submodule of $M$ with $\operatorname{rk} N = n$. If $m \geqq 2n$, then there is a constant $\kappa(M)$ independent of $N$ such that there is a regular submodule $\tilde{N} \supset N$ of $M$ with $\operatorname{rk} \tilde{N} = 2n$ and $\operatorname{ord}_p d\tilde{N} \leqq \kappa(M)$.*

*Proof.* We use the induction on $n$. We may suppose that $B(x, y) \in \boldsymbol{Z}_p$ for all $x, y \in M$ without loss of generality. Suppose that $n = 1$ and $M \cap \boldsymbol{Q}_p N = \boldsymbol{Z}_p v$. Suppose $B(v, M) = B(v, w)\boldsymbol{Z}_p = p^k \boldsymbol{Z}_p$ for $w \in M$; then $p^k$ divides $dM$ since $v$ is primitive. If $p^{2k+1} | Q(v)$, then we put $\tilde{N} = \boldsymbol{Z}_p[v, w]$. It is clear that $\operatorname{ord}_p d\tilde{N} = 2k \leqq 2 \operatorname{ord}_p dM$. If $p^{2k+1} \nmid Q(v)$, then we consider a set

$$S = \{\boldsymbol{Z}_p v' \subset M | \operatorname{ord}_p Q(v') \leqq 2 \operatorname{ord}_p dM\} \qquad (\ni \boldsymbol{Z}_p v) .$$

We can take a finite set $\{\boldsymbol{Z}_p u_i\} \subset S$ such that $S = \bigcup_i O(M) \boldsymbol{Z}_p u_i$. For each $u_i$ we take $w_i \in u_i^{\perp}$ such that $\operatorname{ord}_p Q(w_i) = \min_{w \in u_i^{\perp}} \operatorname{ord}_p Q(w)$, and put $N_i = \boldsymbol{Z}_p[u_i, w_i]$. Then for $v$ there is $w \in M$ such that $\tilde{N} = \boldsymbol{Z}_p[v, w]$ is regular and $\operatorname{ord}_p d\tilde{N} \leqq \max_i \operatorname{ord}_p dN_i$. Thus we can take $\max(2 \operatorname{ord}_p dM, \max_i \operatorname{ord}_p dN_i)$ as $\kappa(M)$ for $n = 1$. Let $N = \boldsymbol{Z}_p[v_1, \cdots, v_n]$ be a submodule of $M$ and $2n \leqq m$. Take $N_1 \subset M$ such that $N_1 \ni v_1$, $\operatorname{ord}_p dN_1 \leqq \kappa_1(M)$ and rank $N_1 = 2$, where $\kappa_1(M)$ is a constant depending only on $M$. Consider a set

$$S' = \{N' \subset M | \operatorname{rank} N' = 2, \operatorname{ord}_p dN' \leqq \kappa_1(M)\} \ni N_1 .$$

Since we can take a finite number of binary submodules $N_i'$ of $M$ such that $S' = \bigcup_i O(M) N_i'$, the set $\{N'^{\perp} | N' \in S'\}$ is a finite set up to $O(M)$ and it depends only on $M$. Decompose $[M: N_1 \perp N_1^{\perp}]v_i$ as $[M: N_1 \perp N_1^{\perp}]v_i = x_i + y_i$, $x_i \in N_1$, $y_i \in N_1^{\perp}$. Since rank $N_1^{\perp} = m - 2$ and $\dim \boldsymbol{Q}_p[y_2, \cdots, y_n] \leqq n - 1 \leqq (m-2)/2$, applying the assumption of the induction, there is a submodule $N_2 \subset N_1^{\perp}$ such that rank $N_2 = 2(n-1)$, $N_2 \ni y_i$ $(i = 2, \cdots, n)$ and $\operatorname{ord}_p dN_2 \leqq \kappa(N_1^{\perp}) \leqq \max_{N' \in S'} \kappa(N'^{\perp}) (= \kappa_2(M)$ say). Put $N' = N_1 \perp N_2$; then

https://doi.org/10.1017/S002776300000252X Published online by Cambridge University Press

rank $N' = 2n$ and $\text{ord}_p\, dN' \leqq \kappa_1(M) + \kappa_2(M)$. Since $N' \ni v_1$, $[M: N_1 \perp N_1^{\perp}]v_i$ $(i \geqq 2)$, $\tilde{N} = M \cap \boldsymbol{Q}_p N'$ contains $N$, rank $\tilde{N} = 2n$ and $\text{ord}_p\, d\tilde{N} \leqq \text{ord}_p\, dN' \leqq \kappa_1(M) + \kappa_2(M)$. Thus we have completed the proof.

LEMMA 2. *Let $M$ be a regular quadratic lattice over $\boldsymbol{Z}_p$ with* rank $M = m$ *and $N$ a regular submodule of $M$ with* rank $N = n$, *and suppose that $m \geqq 2n + 3$. Then there is a constant $\kappa(M)$ dependent only on $M$ satisfying the following condition. Suppose that for a basis $\{v_i\}$ of $N$ $\boldsymbol{Z}_p[v_1, \cdots, v_r]$ is primitive in $M$. Then there are vectors $w_i \in M$ such that*

$$w_i = v_i \qquad \textit{for } 1 \leqq i \leqq r\,,$$
$$B(w_i, w_j) = B(v_i, v_j) \qquad \textit{for } 1 \leqq i, j \leqq n\,,$$
$$[\boldsymbol{Q}_p[w_1, \cdots, w_n] \cap M : \boldsymbol{Z}_p[w_1, \cdots, w_n]] < \kappa(M)\,.$$

*Proof.* We use the induction on $n - r$. Suppose $n - r = 1$. By virtue of the previous lemma, there are vectors $v_1', \cdots, v_{n-1}' \in M$ such that for $N' = \boldsymbol{Z}_p[v_1, \cdots, v_{n-1}, v_1', \cdots, v_{n-1}']$ rank $N'^{\perp} = 2(n-1)$ and $\text{ord}_p\, dN' < \kappa(M)$ hold for some constant $\kappa(M)$. Since rank $N'^{\perp} = m - 2(n-1) \geqq 5$, $N'^{\perp}$ is isotropic. We fix a maximal lattice $K \subset N'^{\perp}$ and decompose $K$ as

$$K = \boldsymbol{Z}_p[e_1, e_2] \perp K_0\,,$$

where $Q(e_1) = Q(e_2) = 0$, $B(e_1, e_2) = p^t$.

Put $v_n = u + a_1 e_1 + a_2 e_2 + z$, where $u \in \boldsymbol{Q}_p N'$, $a_1, a_2, \in \boldsymbol{Q}_p$, $z \in \boldsymbol{Q}_p K_0$. We claim that there are $x_1, x_2 \in \boldsymbol{Z}_p$ such that

$$x_1 x_2 + x_1 a_2 + x_2 a_1 = 0, (x_1 + a_1, x_2 + a_2) \not\subset p\boldsymbol{Z}_p\,.$$

If $a_1 = 0$, then we put $x_1 = 0$ and for some $x_2 \in \boldsymbol{Z}_p$ both conditions are clearly satisfied. The case $a_2 = 0$ is similar. Suppose $a_1 a_2 \neq 0$ and $\text{ord}_p a_1 \leqq \text{ord}_p a_2$. If $a_1 \in \boldsymbol{Z}_p$, then we choose $x_2 \in \boldsymbol{Z}_p$ so that $x_2 + a_2. \in \boldsymbol{Z}_p^{\times}$. Then we have only to put $x_1 = -x_2 a_1 (x_2 + a_2)^{-1}$. If $a_1 \notin \boldsymbol{Z}_p$, $a_2 \in \boldsymbol{Z}_p$, then we have only to put $x_2 = a_2/a_1 \in \boldsymbol{Z}_p$, $x_1 = -x_2 a_1 (x_2 + a_2)^{-1}$, since $x_1 = -(1 + a_1^{-1})^{-1} \in \boldsymbol{Z}_p^{\times}$ and $x_1 + a_1 \notin p\boldsymbol{Z}_p$. If $a_1, a_2 \notin \boldsymbol{Z}_p$, then putting $x_2 = a_1^{-1} \in \boldsymbol{Z}_p$, $x_1 = -(a_1^{-1} + a_2)^{-1} \in \boldsymbol{Z}_p$, we have $x_1 x_2 + x_1 a_2 + x_2 a_1 = 0$ and $x_2 + a_2 \notin \boldsymbol{Z}_p$. Thus we have showed our claim.

Put $w_i = v_i$ for $1 \leqq i \leqq n-1$ and $w_n = v_n + x_1 e_1 + x_2 e_2$; then we have

$$B(v_i, w_n) = B(v_i, v_n) \qquad \text{for } i \leqq n-1\,,$$
$$Q(w_n) = Q(v_n) + B(x_1 e_1 + x_2 e_2, x_1 e_1 + x_2 e_2 + 2v_n)$$
$$= Q(v_n)\,.$$

Thus $B(w_i, w_j) = B(v_i, v_j)$ follows for $1 \leqq i, j \leqq n$. Suppose that for $y \in M$, $p^s y \in \boldsymbol{Z}_p[w_1, \cdots, w_n], p^{s-1}y \notin \boldsymbol{Z}_p[w_1, \cdots, w_n]$ $(s \geqq 1)$; then $p^s y = \sum_{i=1}^{n-1} b_i v_i + b_n w_n = \sum_{i=1}^{n-1} b_i v_i + b_n u + b_n(x_1 + a_1)e_1 + b_n(x_2 + a_2)e_2 + b_n z$ holds. From the assumption $(b_1, \cdots, b_n) = 1$ follows. Since $\boldsymbol{Z}_p[v_1, \cdots, v_{n-1}]$ is primitive in $M$, $b_n$ is in $\boldsymbol{Z}_p^\times$. Since $y \in M$, $[M: N' \perp N'^\perp] y \in N' \perp N'^\perp$ and hence $[M: N' \perp N'^\perp]\,(p^{-s} b_n(x_1 + a_1)e_1 + p^{-s} b_n(x_2 + a_2)e_2 + p^{-s} b_n z) \in N'^\perp$; then $[N'^\perp : K]$ $[M: N' \perp N'^\perp]\,(p^{-s} b_n(x_1 + a_1)e_1 + p^{-s} b_n(x_2 + a_2)e_2) \in \boldsymbol{Z}_p[e_1, e_2]$. Here we note that $\mathrm{ord}_p\, dN' < \kappa(M)$ and $K$ is a fixed maximal lattice in $N'^\perp$, and the number of sumbodule $\tilde{N}$ of $M$ with $\mathrm{ord}_p\, d\tilde{N} < \kappa(M)$ is finite up to $O(M)$ equivalence. Thus $[N'^\perp : K]\,[M: N' \perp N'^\perp] < \kappa_1(M)$ holds for some constant $\kappa_1(M)$ depending only on $M$. From $[N'^\perp : K]\,[M: N' \perp N'^\perp] p^{-s} b_n(x_i + a_i) \in \boldsymbol{Z}_p$ for $i = 1$ and $2$ follows

$$s \leqq \mathrm{ord}_p\,([N'^\perp : K][M: N' \perp N'^\perp](x_i + a_i))\,,$$

since $b_n \in \boldsymbol{Z}_p^\times$.

By the choice of $x_i$, $\mathrm{ord}_p\,(x_i + a_i) \leqq 0$ for $i = 1$ or $2$. Thus there is a constant $\kappa_2(M)$ such that $s \leqq \kappa_2(M)$. Therefore the index $[\boldsymbol{Q}_p[w_1, \cdots, w_n] \cap M: \boldsymbol{Z}_p[w_1, \cdots, w_n]]$ is bounded from above by a constant depending only on $M$.

Suppose $n - r \geqq 2$ and put $N' = \boldsymbol{Q}_p[v_1, \cdots, v_{n-1}] \cap M = \boldsymbol{Z}_p[u_1, \cdots, u_{n-1}]$. We may suppose

(1) $u_i = v_i$ for $1 \leqq i \leqq r$,

since $\boldsymbol{Z}_p[v_1, \cdots, v_r]$ $(\subset N')$ is primitive in $M$.

Applying the assumption of the induction to $N' \oplus \boldsymbol{Z}_p v_n$, there are vectors $u'_i \in M$ such that

(2) $u'_i = u_i$ for $1 \leqq i \leqq n - 1$,
(3) $B(u'_i, u'_j) = B(u_i, u_j)$ for $1 \leqq i, j \leqq n$

where $u_n = v_n$,

(4) $[\boldsymbol{Q}_p[u'_1, \cdots, u'_n] \cap M: \boldsymbol{Z}_p[u'_1, \cdots, u'_n]] < \kappa_1(M)$,

where $\kappa_1(M)$ is a constant depending only on $M$. From (4) follows

(5) $[\boldsymbol{Q}_p[u'_1, \cdots, u'_r, u'_n] \cap M: \boldsymbol{Z}_p[u'_1, \cdots, u'_r, u'_n]] < \kappa_1(M)$.

We choose $v'_n \in M$ so that

(6) $\boldsymbol{Q}_p[u'_1, \cdots, u'_r, u'_n] \cap M = \boldsymbol{Z}_p[v_1, \cdots, v_r, v'_n]$,

https://doi.org/10.1017/S002776300000252X Published online by Cambridge University Press

noting $u'_i = u_i = v_i$ for $i \leqq r$ by (2), (1) and the primitiveness of $\boldsymbol{Z}_p[v_1, \cdots, v_r]$. Putting

(7) $v'_i = v_i$ for $i \leqq n-1$,

$$\begin{aligned} \boldsymbol{Z}_p[v'_1, \cdots, v'_n] &= \boldsymbol{Z}_p[v_{r+1}, \cdots, v_{n-1}] + \boldsymbol{Z}_p[v_1, \cdots, v_r, v'_n] \\ &\supset \boldsymbol{Z}_p[v_{r+1}, \cdots, v_{n-1}] + \boldsymbol{Z}_p[u'_1, \cdots, u'_r, u'_n] \text{ by (6)} \\ &= \boldsymbol{Z}_p[v_1, \cdots, v_{n-1}, u'_n] \text{ by (2), (1)} \end{aligned}$$

and

(8) $[\boldsymbol{Z}_p[v'_1, \cdots, v'_n] \colon \boldsymbol{Z}_p[v_1, \cdots, v_{n-1}, u'_n]] < \kappa_1(M)$

follows from (5).
Put $u = u'_n - u_n$; then for $i \leqq n-1$ we have

$$\begin{aligned} B(u_i, u_n) &= B(u'_i, u'_n) \text{ by (3)} \\ &= B(u_i, u'_n) \text{ by (2)} \end{aligned}$$

and then $B(u_i, u) = 0$ for $i \leqq n-1$.
Since $\boldsymbol{Q}_p[v_1, \cdots, v_{n-1}] = \boldsymbol{Q}_p[u_1, \cdots, u_{n-1}]$, we have $B(v_i, u) = 0$ for $i \leqq n-1$ and hence

$$B(v_i, u'_n) = B(v_i, u_n) = B(v_i, v_n)\,,$$

where the second equality follows from the definition of $u_n = v_n$. Thus we can define an isometry $\sigma$ from $N$ to $\boldsymbol{Z}_p[v_1, \cdots, v_{n-1}, u'_n]$ by

(9) $\begin{cases} \sigma(v_i) = v_i \text{ for } 1 \leqq i \leqq n-1, \\ \sigma(v_n) = u'_n, \end{cases}$

since $Q(u'_n) = Q(u_n) = Q(v_n)$ by (3).
Hence $\dim \boldsymbol{Q}_p[v'_1, \cdots, v'_n] = \dim \boldsymbol{Q}_p[v_1, \cdots, v_{n-1}, u'_n] = n$ follows. By (6), (7) $\boldsymbol{Z}_p[v'_1, \cdots, v'_r, v'_n]$ is primitive in $M$ and $\boldsymbol{Q}_p[v'_1, \cdots, v'_n] = \boldsymbol{Q}_p[v_1, \cdots, v_{n-1}, u'_n] = \boldsymbol{Q}_p\sigma(N)$ is regular. Applying the assumption of the induction to $\boldsymbol{Z}_p[v'_1, \cdots, v'_n]$, there are vectors $w'_i \in M$ such that

(10) $w'_i = v'_i$ for $i = 1, \cdots, r$ and $n$.

$B(w'_i, w'_j) = B(v'_i, v'_j)$ for $1 \leqq i, j \leqq n$.

(11) $[\boldsymbol{Q}_p[w'_1, \cdots, w'_n] \cap M \colon \boldsymbol{Z}_p[w'_1, \cdots, w'_n]] < \kappa_1(M)$.

Defining an isometry $\eta$ by $\eta(v'_i) = w'_i$ for $1 \leqq i \leqq n$, we have a submodule $\eta\sigma(N)$ of $M$ since

https://doi.org/10.1017/S002776300000252X Published online by Cambridge University Press

$$Z_p[v_1, \cdots, v_{n-1}, u'_n] \subset Z_p[v'_1, \cdots, v'_n] .$$

Moreover we have, by (9), (7), (10)

$$\eta\sigma(v_i) = v_i \qquad \text{for } i \leqq r .$$

Now we put $w_i = \eta\sigma(v_i)$ for $1 \leqq i \leqq n$; then

$$w_i = v_i \qquad \text{for } i \leqq r ,$$
$$B(w_i, w_j) = B(v_i, v_j) \qquad \text{for } 1 \leqq i, j \leqq n$$

hold.

Finally we have

$$\begin{aligned}
&[\boldsymbol{Q}_p[w_1, \cdots, w_n] \cap M \colon Z_p[w_1, \cdots, w_n]] \\
&\quad = [\boldsymbol{Q}_p[w'_1, \cdots, w'_n] \cap M \colon \eta\sigma(N)] \\
&\quad = [\boldsymbol{Q}_p[w'_1, \cdots, w'_n] \cap M \colon Z_p[w'_1, \cdots, w'_n]][Z_p[w'_1, \cdots, w'_n] \colon \eta\sigma(N)] \\
&\quad < \kappa_1(M)[Z_p[v'_1, \cdots, v'_n] \colon \sigma(N)] \text{ by (11)} \\
&\quad = \kappa_1(M)[Z_p[v'_1, \cdots, v'_n] \colon Z_p[v_1, \cdots, v_{n-1}, u'_n]] \text{ by (9)} \\
&\quad < \kappa_1(M)^2 \text{ by (8)} .
\end{aligned}$$

Thus we have completed the proof.

LEMMA 3. *Let $M$ be a regular quadratic lattice over $Z_p$ and $N$ a regular submodule of $M$ with* rank $M \geqq 2$ rank $N + 3$. *For a natural number $a$ there is a constant $\kappa(M, a)$ dependent only on $M$ and $a$ satisfying the following condition. There is an isometry $\sigma$ from $N$ to $M$ such that*

$$\sigma(x) \equiv x \bmod p^a M \qquad \textit{for } x \in N ,$$
$$[\boldsymbol{Q}_p\sigma(N) \cap M \colon \sigma(N)] < \kappa(M, a) .$$

*Proof.* We take a basis $\{v_i\}$ of $N$ such that

$$\boldsymbol{Q}_p N \cap M = Z_p[p^{-a_1}v_1, \cdots, p^{-a_n}v_n]$$

with $0 \leqq a_1 \leqq \cdots \leqq a_r < a \leqq a_{r+1} \leqq \cdots \leqq a_n$. Define $u_i$ by

$$u_i = \begin{cases} p^{-a_i}v_i \text{ for } i \leqq r , \\ p^{-a}v_i \text{ for } i > r . \end{cases}$$

By virtue of the previous lemma, there are vectors $w_i \in M$ such that

$$w_i = u_i = p^{-a_i}v_i \qquad \text{for } i \leqq r$$
$$B(w_i, w_j) = B(u_i, u_j)$$
$$[\boldsymbol{Q}_p[w_1, \cdots, w_n] \cap M \colon Z_p[w_1, \cdots, w_n]] < \kappa(M) ,$$

where $\kappa(M)$ is a constant dependent only of $M$.

Put $z_i = p^{a_i}w_i$ for $i \leqq r$ and $z_i = p^a w_i$ for $i > r$; then we have $B(v_i, v_j) = B(z_i, z_j)$,

$$z_i = v_i \qquad \text{for } i \leqq r\,,$$
$$z_i \equiv v_i \equiv 0 \bmod p^a M \qquad \text{for } i > r\,.$$

Moreover

$$\begin{aligned}
&[\boldsymbol{Q}_p[z_1, \cdots, z_n] \cap M : \boldsymbol{Z}_p[z_1, \cdots, z_n]] \\
&\quad = [\boldsymbol{Q}_p[w_1, \cdots, w_n] \cap M : \boldsymbol{Z}_p[w_1, \cdots, w_n]] \\
&\qquad \times [\boldsymbol{Z}_p[w_1, \cdots, w_n] : \boldsymbol{Z}_p[z_1, \cdots, z_n]] \\
&\quad = p^{\sum_{i=1}^r a_i + (n-r)a} [\boldsymbol{Q}_p[w_1, \cdots, w_n] \cap M : \boldsymbol{Z}_p[w_1, \cdots, w_n]] \\
&\quad \leqq p^{na}\kappa(M)\,.
\end{aligned}$$

We have only to put $\sigma(v_i) = z_i$ and $\kappa(M, a) = p^{na}\kappa(M)$.

Now we can prove Proposition. Let $S, T, P, a$ be those at the beginning of this section, and suppose $\alpha_p(S, T; P, p^a) \neq 0$; then there is $X \in M_{m,n}(\boldsymbol{Z}_p)$ such that $S[X] = T, X \equiv P \bmod p^a$. By virtue of Lemma 3 there is $Y \in M_{m,n}(\boldsymbol{Z}_p)$ such that $Y \equiv P \bmod p^a$, $S[Y] = T$ and for elementary divisors $p^{a_1}, \cdots, p^{a_n}$ of $Y$ $\sum_{i=1}^n a_i < \kappa(S, a)$ holds where $\kappa(S, a)$ is a constant independent of $T$. Take a natural number $b$ larger than $a, a_i$ $(1 \leqq i \leqq n)$. Clearly $\alpha_p(S, T; P, p^a) \geqq \alpha_p(S, T; Y, p^b) \neq 0$ holds. Let

$$Y = U \begin{pmatrix} p^{a_1} & & \\ & \ddots & \\ & & p^{a_n} \\ & 0 & \end{pmatrix} V,\ U \in GL_m(\boldsymbol{Z}_p),\ V \in GL_n(\boldsymbol{Z}_p)$$

and put $U^{-1}Y = \begin{pmatrix} A \\ 0 \end{pmatrix}$, $A = \operatorname{diag}(p^{a_1}, \cdots, p^{a_n})V \in M_{n,n}(\boldsymbol{Z}_p)$. $S[Y] = T$ implies $S[YA^{-1}] = T[A^{-1}]$ and hence $T[A^{-1}]$ is integral since $YA^{-1} = U\begin{pmatrix} 1_n \\ 0 \end{pmatrix}$. We consider the mapping $X \mapsto XA$ from

$$\left\{ X \in M_{m,n}(\boldsymbol{Z}_p) \bmod p^t \,\middle|\, \begin{array}{l} S[X] \equiv T[A^{-1}] \bmod p^t \\ X \equiv U\begin{pmatrix} 1_n \\ 0 \end{pmatrix} \bmod p^b \end{array} \right\}$$

to

$$\left\{ Z \in M_{m,n}(\boldsymbol{Z}_p) \bmod p^t M_{m,n}(\boldsymbol{Z}_p)A \,\middle|\, \begin{array}{l} S[Z] \equiv T \bmod p^t \\ Z \equiv Y \bmod p^b \end{array} \right\}.$$

https://doi.org/10.1017/S002776300000252X Published online by Cambridge University Press

It is obviously well-defined and injective.
Hence we have

$$\alpha_p(S, T;\ Y, p^b) \geqq |A|^{-m}\alpha_p\Big(S,\ T[A^{-1}];\ U\binom{1_n}{0}, p^b\Big) \neq 0\,.$$

The last inequality follows from $S[YA^{-1}] = T[A^{-1}]$, $YA^{-1} = U\binom{1_n}{0}$. Next we have

$$\#\Big\{X \in M_{m,n}(\boldsymbol{Z}_p) \bmod p^t \,\Big|\, S[X] \equiv T[A^{-1}] \bmod p^t,\ X \equiv U\binom{1_n}{0} \bmod p^b\Big\}$$

$$\geqq p^{-mn}\#\left\{X \in M_{m,n}(\boldsymbol{Z}_p) \bmod p^{t+1} \,\middle|\, \begin{array}{l} S[Xx] \equiv T[A^{-1}][x] \bmod p^{t+1} \\ \text{for every } x \in M_{n,1}(\boldsymbol{Z}_p), \\ X \equiv U\binom{1_n}{0} \bmod p^b \end{array}\right\}$$

by considering the canonical mapping from the latter set to the former set,

$$= p^{-mn+n\,\mathrm{ord}_p|S|}$$

$$\times \#\left\{X \in M_{m,n}(\boldsymbol{Z}_p) \bmod p^{t+1}S^{-1}M_{m,n}(\boldsymbol{Z}_p) \,\middle|\, \begin{array}{l} S[Xx] \equiv T[A^{-1}][x] \bmod p^{t+1} \\ \text{for every } x \in M_{n,1}(\boldsymbol{Z}_p), \\ X \equiv U\binom{1_n}{0} \bmod p^b \end{array}\right\}$$

for a sufficiently large $t$.
By virtue of "Satz" in Section 14 in [5]

$$(p^{t+1})^{n(n+1)/2-mn}$$

$$\times \#\left\{X \in M_{m,n}(\boldsymbol{Z}_p) \bmod p^{t+1}S^{-1}M_{m,n}(\boldsymbol{Z}_p) \,\middle|\, \begin{array}{l} S[Xx] \equiv T[A^{-1}][x] \bmod p^{t+1} \\ \text{for every } x \in M_{n,1}(\boldsymbol{Z}_p), \\ X \equiv U\binom{1_n}{0} \bmod p^b \end{array}\right\}$$

is constant if $t$ is larger than some constant $t_0$ which depends only on $S$ and $b$. Thus we have

$$\alpha_p\Big(S,\ T[A^{-1}];\ U\binom{1_n}{0}, p^b\Big) \geqq p^{-mn+n\,\mathrm{ord}_p|S|+t_0(n(n+1)/2-mn)}\,,$$

since $S[YA^{-1}] = T[A^{-1}]$ and $YA^{-1} = U\binom{1_n}{0}$.

Noting that $|A|^{-m} = p^{-m(\Sigma a_i)} \geqq p^{-m\kappa(S,a)}$, we complete the proof.

https://doi.org/10.1017/S002776300000252X Published online by Cambridge University Press

§ 4.

Let $S$ be an integral symmetric positive definite matrix of degree $m$ whose diagonals are even integers and $n$ a natural number with $m \geqq 2n + 3$, and we take $P \in M_{m,n}(\boldsymbol{Z})$ and a natural number $\nu$. Let $\theta(Z, S, -P, \nu)$, $E(Z, S, -P, \nu)$ be Siegel modular forms of level $q\nu^2$, weight $m/2$ and degree $n$ defined in Section 2, where $q$ is the level of $S$, and put

$$\theta(Z, S, -P, \nu) = \sum_{T \geqq 0} A(S, T;\ P, \nu) \exp(\pi i \operatorname{tr} TZ)\,,$$
$$E(Z, S, -P, \nu) = \sum_{T \geqq 0} A_0(S, T; P, \nu) \exp(\pi i \operatorname{tr} TZ)\,,$$

where $A(S, T; P, \nu)$ and $A_0(S, T; P, \nu)$ are the same as those defined in Section 1 for every positive definite matrix $T$. As pointed out in Section 2 for $a(T) = A(S, T; P, \nu) - A_0(S, T; P, \nu)$ $\sum a(T) \exp(\pi i \operatorname{tr} TZ)$ is a Siegel modular form of weight $m/2$, degree $n$ such that the constant term at every cusp vanishes.

Denote by $A_{\mathrm{pr}}(S, T; P, \nu)$ the number of $X \in M_{m,n}(\boldsymbol{Z})$ such that $S[X] = T$, $X \equiv P \bmod \nu$ and $X$ is primitive in $M_{m,n}(\boldsymbol{Z}_p)$ for $p \nmid \nu$ and put $A_{0,\mathrm{pr}}(S, T; P, \nu) = M(S, \nu)^{-1} \sum_{\mathfrak{P}\mathfrak{S}(S,\nu)/\tilde{\nu} \ni S'} (A_{\mathrm{pr}}(S', T; P, \nu)/E(S', \nu))$, and $a_{\mathrm{pr}}(T) = A_{\mathrm{pr}}(S, T; p, \nu) - A_{0,\mathrm{pr}}(S, T; P, \nu)$. Our aim is to get an asymptotic formula for $A_{\mathrm{pr}}(S, T; P, \nu)$. Let $V = \boldsymbol{Q}[v_1, \cdots, v_m]$, $W = \boldsymbol{Q}[w_1, \cdots, w_n]$ be quadratic space with bilinear forms defined by $(B(v_i, v_j)) = S$, $(B(w_i, w_j)) = T$ respectively, and $\sigma_0$ a linear mapping from $W$ to $V$ defined by

$$(\sigma_0(w_1), \cdots, \sigma_0(w_n)) = (v_1, \cdots, v_m)P\,.$$

It is clear, then, that $A(S, T; P, \nu)$ is the number of isometries $\sigma$ from $W$ to $V$ such that $\sigma N \subset M$ and $\sigma(x) \equiv \sigma_0(x) \bmod \nu \boldsymbol{Z}_p M$ for all $x$ in $\boldsymbol{Z}_p N$ for every prime $p$ where we put $M = \boldsymbol{Z}[v_1, \cdots, v_m]$, $N = \boldsymbol{Z}[w_1, \cdots, w_n]$. $A_{\mathrm{pr}}(S, T; P, \nu)$ is the number of isometries $\sigma$ with an additional condition that $\sigma(\boldsymbol{Z}_p N)$ is primitive in $\boldsymbol{Z}_p M$ for $p \nmid \nu$. We write $A(M, N; \sigma_0, \nu)$, $A_{\mathrm{pr}}(M, N; \sigma_0, \nu)$ for $A(S, T; P, \nu)$, $A_{\mathrm{pr}}(S, T; P, \nu)$ respectively. Obviously we have

$$A(M, N; \sigma_0, \nu) = \sum_{L \supset N} A_{\mathrm{pr}}(M, L; \sigma_0, \nu)\,,$$

where $L$ runs over submodules of $W$ such that $L \supset N$ and $\boldsymbol{Z}_p L = \boldsymbol{Z}_p N$ for $p \mid \nu$. Similarly putting

$$A_0(M, N; \sigma_0, \nu) = A_0(S, T; P, \nu)\,,$$
$$A_{0,\mathrm{pr}}(M, N; \sigma_0, \nu) = A_{0,\mathrm{pr}}(S, T; P, \nu)\,,$$

we have

$$(\sharp) \qquad A_0(M, N; \sigma_0, \nu) = \sum_{L \supset N} A_{0,\mathrm{pr}}(M, L; \sigma_0, \nu)$$

where $L$ runs over the same set as above. Using the theory of Hecke algebra of $GL$ as in [4], we have

$$A_{\mathrm{pr}}(M, N; \sigma_0, \nu) = \sum_{L \supset N} \pi(L, N) A(M, L; \sigma_0, \nu)\,,$$
$$A_{0,\mathrm{pr}}(M, N; \sigma_0, \nu) = \sum_{L \supset N} \pi(L, N) A_0(M, L; \sigma_0, \nu)\,,$$

where $L$ runs over lattices of $\boldsymbol{Q}N$ containing $N$ such that $\boldsymbol{Z}_pL = \boldsymbol{Z}_pN$ for $p|\nu$, and $\pi(L, N)$ is defined as follows: Suppose that $\boldsymbol{Z}_pL/\boldsymbol{Z}_pN$ is isomorphic to $h_p$ copies of $\boldsymbol{Z}_p/p\boldsymbol{Z}_p$ as $\boldsymbol{Z}_p$ modules for every prime $p$; then we put

$$\pi(L, N) = \prod_p (-1)^{h_p} p^{h_p(h_p-1)/2}\,.$$

Otherwise we put $\pi(L, N) = 0$. For a lattice $L$ in $\boldsymbol{Q}N$ such that

$$L \supset N \text{ and } \boldsymbol{Z}_pL = \boldsymbol{Z}_pN \text{ for } p|\nu\,,$$

we take a basis $\{w'_i\}$ such that $w'_i \equiv w_i \bmod \nu\boldsymbol{Z}_pN$ for $p|\nu$ and put $T_L = (B(w'_i, w'_j))$. It is clear that $A(S, T_L; P, \nu) = A(M, L; \sigma_0, \nu)$, and hence we have

$$a_{\mathrm{pr}}(T) = \sum_{L \supset N} \pi(L, N) a(T_L)\,,$$

where $L$ runs over the same set as above.

Suppose that

$$(*) \qquad a(T) = O((\min T)^{-\varepsilon} |T|^{(m-n-1)/2})$$

for every positive definite matrix $T \in M_{n,n}(\boldsymbol{Z})$, where $\min T = \min_{0 \neq x \in \boldsymbol{Z}^n} T[x]$ and $\varepsilon$ is a sufficiently small positive number. This is the case for $n = 2$. We have, then as in [4]

$$a_{\mathrm{pr}}(T) = O((\min T)^{-\varepsilon} |T|^{(m-n-1)/2})\,.$$

Thus we have

$$(\sharp\sharp) \qquad A_{\mathrm{pr}}(S, T; P, \nu) = A_{0,\mathrm{pr}}(S, T; P, \nu) + O((\min T)^{-\varepsilon} |T|^{(m-n-1)/2})$$

for every positive definite integral matrix $T$ under the assumption $(*)$ which is true for $n = 2$.

We denote by $A'_{0,\mathrm{pr}}(S, T; P, \nu)$ the right side of the formula for $A_0(S, T; P, \nu)$ in Theorem of Section 1 in which $\alpha_p(S, T; P, \nu)$ is replaced by

$$2^{-\delta_{m,n}} \lim_{a\to\infty} (p^a)^{n(n+1)/2-mn} \# \left\{ X \in M_{m,n}(Z_p/p^a Z_p) \middle| \begin{array}{l} S[X] \equiv T \bmod p^a Z_p, \\ X \text{ is primitive} \end{array} \right\}$$

for $p \nmid \nu$. By virtue of Hilfssatz 13 in [7], the identity (♯) holds for $A'_{0,\mathrm{pr}}$ instead of $A_{0,\mathrm{pr}}$. Hence the inversion formula in [4] implies $A'_{0,\mathrm{pr}} = A_{0,\mathrm{pr}}$. By virtue of Proposition in Section 3 there is a positive constant $\kappa$ independent of $T$ such that

$$A_{0,\mathrm{pr}}(S, T; P, \nu) > \kappa |T|^{(m-n-1)/2}$$

if $T > 0$ and $A_{0,\mathrm{pr}}(S, T; P, \nu) \neq 0$, using an argument of the proof of Proposition 9 in [3] with $A'_{0,\mathrm{pr}} = A_{0,\mathrm{pr}}$. Thus we have proved the following

THEOREM. *Let $S$ be a positive definite integral matrix of degree $m$ whose diagonals are even and $n$ a natural number with $m \geqq 2n + 3$. We take $P \in M_{m,n}(Z)$ and a natural number $\nu$. Then there exists positive numbers $\kappa, \varepsilon$ such that*

$$A_{\mathrm{pr}}(S, T; P, \nu) = A_{0,\mathrm{pr}}(S, T; P, \nu) + O((\min T)^{-\varepsilon} |T|^{(m-n-1)/2}),$$
$$A_{0,\mathrm{pr}}(S, T; P, \nu) > \kappa |T|^{(m-n-1)/2} \qquad \text{if } A_{0,\mathrm{pr}}(S, T; P, \nu) \neq 0,$$

*for every positive definite integral matrix $T$ of degree $n$, provided $n = 2$.*

Immediately we have

COROLLARY. *Let $M' \subset M$ be positive definite quadratic lattices over $Z$ of rank $m \geqq 2n + 3$, $S$ a finite set of primes containing all prime divisors of $2[M: M']$ and such that $M_p$ is unimodular for $p \notin S$. There is a constant $c$ such that for every positive definite quadratic lattice $N$ of rank $n$ and every collection $(f_p)_{p\in S}$ of isometries $f$: $Z_pN \to Z_pM$ there is an isometry $f$: $N \to M$ satisfying*

$$f \equiv f_p \bmod Z_pM' \qquad \text{for every } p \in S,$$
$$f(Z_pN) \text{ is primitive in } Z_pM \text{ for every } p \notin S,$$

*if $\min_{0\neq x\in N} Q(x) > c$, provided $n = 2$.*

## REFERENCES

[1] A. N. Andrianov and G. N. Maloletkin, Behavior of theta series of degree $n$ under modular substitutions, Math. USSR-Izv., **9** (1975), 227–241.
[2] J. S. Hsia, Y. Kitaoka and M. Kneser, Representations of positive definite quadratic forms, J. reine angew. Math., **301** (1978), 132–141.
[3] Y. Kitaoka, Modular forms of degree $n$ and representation by quadratic forms II, Nagoya Math. J., **87** (1982), 127–146.

[4] ——, Lectures on Siegel modular forms and representation by quadratic forms, Tata Institute Lectures on Math., Springer-Verlag (1986).
[5] M. Kneser, Quadratische Formen, Vorlesungs Ausarbeitung, Göttingen (1973/4).
[6] O. T. O'Meara, Introduction to quadratic forms, Springer-Verlag (1963).
[7] C. L. Siegel, Über die analytische Theorie der quadratischen Formen, Ann. of Math., **36** (1935), 527–606.
[8] F. van der Blij, On the theory of quadratic forms, Ann. of Math., **50** (1949), 875–883.