Y. Kitaoka
Nagoya Math. J.
Vol. 133 (1994), 127–153

THE MINIMUM AND THE PRIMITIVE REPRESENTATION OF POSITIVE DEFINITE QUADRATIC FORMS

YOSHIYUKI KITAOKA

Let M, N be positive definite quadratic lattices over $\mathbf{Z}$ with $\operatorname{rank}(M) = m$ and $\operatorname{rank}(N) = n$ respectively. When there is an isometry from M to N, we say that M is represented by N (even in the local cases). In the following, we assume that the localization M_p is represented by N_p for every prime p. Let us consider the following assertion $\mathrm{A}_{m,n}(N)$:

$\mathrm{A}_{m,n}(N)$: *There exists a constant $c(N)$ dependent only on N so that M is represented by N if $\min(M) > c(N)$, where $\min(M)$ denotes the least positive number represented by M.*

We know that this is true if $n \geq 2m + 3$, and a natural problem is whether the condition $n \geq 2m + 3$ is the best or not. It is known that this is the best if $m = 1$. But in the case of $m \geq 2$, what we know at present, is that there is an example N so that $\mathrm{A}_{m,n}(N)$ is false if $n - m = 3$. We do not know such examples when $n - m = 4$. Anyway, analyzing the counter-example, we come to the following two assertions $\mathrm{APW}_{m,n}(N)$ and $\mathrm{R}_{m,n}(N)$.

$\mathrm{APW}_{m,n}(N)$: *There exists a constant $c'(N)$ dependent only on N so that M is represented by N if $\min(M) > c'(N)$ and M_p is primitively represented by N_p for every prime p.*

$\mathrm{R}_{m,n}(N)$: *There is a lattice M' containing M such that M'_p is primitively represented by N_p for every prime p and $\min(M')$ is still large if $\min(M)$ is large.*

If the assertion $\mathrm{R}_{m,n}(N)$ is true, then the assertion $\mathrm{A}_{m,n}(N)$ is reduced to the apparently weaker assertion $\mathrm{APW}_{m,n}(N)$. If the assertion $\mathrm{R}_{m,n}(N)$ is false, then it becomes possible to make a counter-example to the assertion $\mathrm{A}_{m,n}(N)$. As a matter of fact, the assertion $\mathrm{R}_{m,m+3}(N)$ is false in a certain kind of lattices N and it yields examples of N such that the assertion $\mathrm{A}_{m,m+3}(N)$ is false. Note that $\mathrm{APW}_{1,4}(N)$ is true for every N although $A_{1,4}(N)$ is false in general.

We proved in [4] that the assertion $\mathrm{R}_{m,2m+2}(N)$ is true if $m \geq 2$. The aim of this paper is to show that the assertion $\mathrm{R}_{m,2m+1}(N)$ is also true if $m \geq 3$ (Theorem

Received June 15, 1993.

in §2).
To what extent is the assertion $R_{m,n}(N)$ is true?
In §3, we give some remarks on the asymptotic formula for the number of isometries from M to N.

We denote by $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{Z}_p$ and $\mathbf{Q}_p$ the ring of integers, the field of rational numbers and their p-adic completions.

Terminology and notation on quadratic forms are those from [5], [6]. For a lattice M on a quadratic space V over $\mathbf{Q}$, the scale $s(M)$ denotes $\{B(x, y) \mid x, y \in M\}$. Even for the localization M_p it is similarly defined. dM, dM_p denote the discriminant of M, M_p respectively.
For a subset S of a positive definite quadratic space V, we put

$$\min(S) = \min_Q(S) := \min\{Q(x) \mid 0 \neq x \in S\}.$$

For a matrix A, ${}^tA$ denotes the transposed matrix of A.
For square matrices $A_1, \ldots, A_n$, $\mathrm{diag}(A_1, \ldots, A_n)$ means $\begin{pmatrix} A_1 & & \\ & \ddots & \\ & & A_n \end{pmatrix}$.

§1

The aim of this section is to prove the following preparatory theorem.

THEOREM. *Let m be a natural number (≥ 3), p a prime number and M a lattice on a positive definite quadratic space V over $\mathbf{Q}$ with $\dim V = m$, $s(M) \subset \mathbf{Z}$ and $s(M_p) = \mathbf{Z}_p$. Suppose that there is a basis $\{w_1, \ldots, w_m\}$ of M such that*

$$(B(w_i, w_j)) \equiv \mathrm{diag}(\varepsilon, B_1 p^{a_1}, \ldots, B_u p^{a_u}) \mod p^{2a_u},$$

where $\varepsilon \in \mathbf{Z}_p^\times$, B_i is even unimodular for $1 \leq i \leq u$ with $(1,1)$-entry not divisible by $2p$ and $2 < a_1 < \cdots < a_u$. Put $s := [a_1/2]$ where $[x]$ is the largest integer not exceeding x. Let κ be a real number with $0 < \kappa < 1/7$. Then there is a positive constant C independent of M but dependent on m, κ and p, which satisfies the following: If we have the inequality

$$\min(M) > C,$$

then there is an element w of M so that $w = \sum_{i=2}^m f_i w_i \in M$ whth $f_2 \not\equiv 0 \mod p$, and $f_3 \equiv \cdots \equiv f_m \equiv 0 \mod p$, and w satisfies the followings:

(i) $\min(M + p^{-s}\mathbf{Z}[w]) \geq \min(M)^\kappa$.

(ii) $s(M + p^{-s}\mathbf{Z}[w]) \subset \mathbf{Z}$.

https://doi.org/10.1017/S0027763000004773 Published online by Cambridge University Press

(iii) $\mathrm{ord}_p(d(\mathbf{Z}[w_1, p^{-s}w])) \leq 2$.

The assertions (ii) and (iii) are satisfied for every f of the above form and so the rest of this section is devoted to prove the assertion (i).
Throughout this section, m, p, κ, s and M denote those given in Theorem.

DEFINITION For a real number x, we define the decimal part $\lceil x \rceil$ by the conditions

$$-1/2 \leq \lceil x \rceil < 1/2 \quad \text{and} \quad x - \lceil x \rceil \in \mathbf{Z}.$$

LEMMA 1. *Let q_1, q_2 and K be positive numbers. If an integer u satisfies the following inequalities* (1) *and* (2):

$$\min_{p^s \nmid b} (\lceil bp^{-s} \rceil^2 q_1 + \lceil bup^{-s} \rceil^2 q_2) < K, \tag{1}$$

where b runs over the set of integers not divisible by p^s,

$$\frac{1}{4}\sqrt{q_1/K} < |u| < \frac{1}{2}\sqrt{q_1/K}, \tag{2}$$

then we have

$$q_1 q_2 \leq 16K^2 p^{2s}. \tag{3}$$

Proof. We note that $\lceil bp^{-s} \rceil$ depends only on $b \bmod p^s$. So we may suppose that an integer b with $0 \neq |b| \leq p^s/2$ gives the minimum of the left-hand side of the inequality (1). Then we have $K > \lceil bp^{-s} \rceil^2 q_1 = b^2 p^{-2s} q_1$ and so the inequality $|b| < \sqrt{K/q_1}\, p^s$. The condition (2) implies, then the inequality $|bu| < p^s/2$ and so $K > \lceil bup^{-s} \rceil^2 q_2 = b^2 u^2 p^{-2s} q_2 \geq u^2 q_2 p^{-2s} \geq q_1 q_2/(16K) \cdot p^{-2s}$, which is nothing but the inequality (3). □

LEMMA 2. *Let q_1, q_2 and K be positive numbers and u_0 an integer. Suppose that a natural number e satisfies an inequality*

$$p^e < \frac{1}{4}\sqrt{q_1/K}.$$

If the inequality (1) *holds for every integer u with $u \equiv u_0 \bmod p^e$, then we have the inequality* (3).

https://doi.org/10.1017/S0027763000004773 Published online by Cambridge University Press

Proof. By the inequality $\frac{1}{2}\sqrt{q_1/K} - \frac{1}{4}\sqrt{q_1/K} > p^e$, we can take an integer u so that $\frac{1}{4}\sqrt{q_1/K} < u < \frac{1}{2}\sqrt{q_1/K}$ and $u \equiv u_0 \bmod p^e$. The assertion follows immediately from Lemma 1. $\square$

LEMMA 3. *Let* $\{v_1, \ldots, v_m\}$ *be a basis of* M. *Suppose* $(B(v_i, v_j)) = \mathrm{diag}(q_1, \ldots, q_m) > 0$. *For an element* $w := \sum_{i=1}^m r_i v_i \in M$, *we have*

$$\min(M + p^{-s}\mathbf{Z}[w]) = \min_{\substack{b \in \mathbf{Z} \\ bw \notin p^s M}} \left(\sum_{i=1}^m \lceil b r_i p^{-s} \rceil^2 q_i\right)$$

if $\min(M + p^{-s}\mathbf{Z}[w]) < \min(M)$.

Proof. Suppose that $y = x + p^{-s}bw$ $(x \in M,\ b \in \mathbf{Z})$ gives the minimum $\min(M + p^{-s}\mathbf{Z}[w])$. If $bw \in p^s M$, then $y \in M$ follows and this contradicts $\min(M + p^{-s}\mathbf{Z}[w]) < \min(M)$. Thus we have $bw \notin p^s M$. Moreover putting $x = \sum_{i=1}^m x_i v_i$ $(x_i \in \mathbf{Z})$, the minimality implies

$$Q(y) = \sum_{i=1}^m (x_i + b r_i p^{-s})^2 q_i = \sum_{i=1}^m \lceil b r_i p^{-s} \rceil^2 q_i,$$

which completes the proof. $\square$

DEFINITION. For a positive numbers a, b, we write

$$a \ll b$$

if there is a positive number c dependent only on $m = \mathrm{rank}\, M$ such that $a/b < c$. If both $a \ll b$ and $b \ll a$ hold, then we write

$$a \asymp b.$$

LEMMA 4. *Let* $\{v_1, \ldots, v_m\}$ *and* $\{w_1, \ldots, w_m\}$ *be bases of* M *such that* $(B(v_i, v_j))$ *is reduced in the sense of Minkowski. We define an element* $A \in GL_m(\mathbf{Z})$ *by*

$$(w_1, \ldots, w_m) := (v_1, \ldots, v_m)A.$$

For an element $w := \sum_{i=1}^m f_i w_i \in M$, *we define integers* r_i *by*

$${}^t(r_1, \ldots, r_m) := A^t(f_1, \ldots, f_m).$$

Then there is a positive constant c_1 *dependent only on* m *so that*

https://doi.org/10.1017/S0027763000004773 Published online by Cambridge University Press

$$\min(M + \mathbf{Z}[p^{-s}w]) \asymp \min_{\substack{b\in\mathbf{Z} \\ bw\notin p^sM}} \left(\sum_{i=1}^m \lceil br_i p^{-s}\rceil^2 Q(v_i)\right)$$

if

$$\min(M + \mathbf{Z}[p^{-s}w]) < c_1 \min(M). \tag{4}$$

Proof. By reduction theory, we know that there exist positive constant c_2, c_3 which depend only on m so that

$$c_2 \sum_{i=1}^m x_i^2 Q(v_i) \le Q(\sum_{i=1}^m x_i v_i) \le c_3 \sum_{i=1}^m x_i^2 Q(v_i) \quad \text{for} \quad x_i \in \mathbf{R}. \tag{5}$$

We introduce a new quadratic form Q' on M defined by

$$Q'(\sum_{i=1}^m x_i v_i) := \sum_{i=1}^m x_i^2 Q(v_i).$$

Putting $c_1 := c_2/c_3$, the assumption (4) and the inequalities (5) imply

$$\begin{aligned}\min_{Q'}(M + \mathbf{Z}[p^{-s}w]) &\le c_2^{-1} \min_Q(M + \mathbf{Z}[p^{-s}w]) \le c_3^{-1} \min_Q(M) \\ &\le \min_{Q'}(M).\end{aligned}$$

Because of $w = \sum_{i=1}^m r_i v_i$, Lemma 3 implies

$$\min_{Q'}(M + p^{-s}\mathbf{Z}[w]) = \min_{\substack{b\in\mathbf{Z} \\ bw\notin p^s\mathbf{Z}}} \left(\sum_{i=1}^m \lceil br_i p^{-s}\rceil^2 Q(v_i)\right).$$

Moreover the inequalities (5) yield

$$\min_Q(M + p^{-s}\mathbf{Z}[w]) \asymp \min_{Q'}(M + p^{-s}\mathbf{Z}[w]),$$

which completes the proof with the above equality. □

LEMMA 5. *Let a matrix $A = (a_{ij})$ be an element of $GL_m(\mathbf{Z})$. Suppose $a_{\alpha 2} \not\equiv 0 \bmod p$ $(1 \le \alpha \le m)$. Then there is an integer β with $1 \le \beta \le m$ and $\beta \ne \alpha$ so that for given integers k_i $(1 \le i \le m)$ with $k_\alpha = 0$, there exists a vector $x = {}^t(x_1, \ldots, x_m) \in \mathbf{Z}^m$ $(x_1 = 0)$ satisfying*

$$g_i \equiv k_i \bmod p^{s-1} \quad \textit{for} \quad i \ne \beta,$$

where we put ${}^t(g_1, \ldots, g_m) := Ax$.

https://doi.org/10.1017/S0027763000004773 Published online by Cambridge University Press

Proof. If $s = 1$, then the assertion is clear and so we may assume $s \geq 2$. Denote by A_i the i-th column vector of A and take integers b_i so that $a_{\alpha i} \equiv b_i a_{\alpha 2} \bmod p^{s-1}$. The equation

$$A \begin{pmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & -b_3 & -b_4 & \cdots & -b_m \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ \vdots & & & \ddots & & \vdots \\ 0 & & & \cdots & & 1 \end{pmatrix}$$
$$= (A_1, A_2, A_3 - b_3 A_2, \ldots, A_m - b_m A_2)$$

implies that there is an $(m-2) \times (m-2)$ submatrix of

$$\tilde{A} := (A_3 - b_3 A_2, \ldots, A_m - b_m A_2)$$

whose determinant is not divisible by p. Since the α-th row of $\tilde{A}$ is congruent to 0 modulo p^{s-1}, there is an integer β $(\neq \alpha)$ such that the determinant of the submatrix of $\tilde{A}$ which misses α and β-th rows from the matrix $\tilde{A}$ is not divisible by p. Let $T \in GL_m(\mathbf{Z})$ be a matrix so that its multiplication from the left induces the interchange of α (resp. β)-th row and the first (resp. second) row. Then the lower $(m-2) \times (m-2)$ submatrix C of $T\tilde{A}$ is regular modulo p. Now we define integers $x_3, \ldots, x_m$ by

$$C\,{}^t(x_3, \ldots, x_m) \equiv {}^t(k'_3, \ldots, k'_m) \bmod p^{s-1},$$

where we put ${}^t(k'_1, \ldots, k'_m) := T\,{}^t(k_1, \ldots, k_m)$. Then we have

$$T\Big(\sum_{i=3}^{m} x_i (A_i - b_i A_2)\Big) = T\tilde{A}\,{}^t(x_3, \ldots, x_m)$$
$$\equiv \begin{pmatrix} 0 \cdots 0 \\ * \cdots * \\ C \end{pmatrix} \begin{pmatrix} x_3 \\ \vdots \\ x_m \end{pmatrix} \equiv \begin{pmatrix} 0 \\ * \\ k'_3 \\ \vdots \\ k'_m \end{pmatrix} \bmod p^{s-1}.$$

Hence, putting $x_2 := -\sum_{i=3}^{m} b_i x_i$, $x_1 = 0$ and $x := {}^t(x_1, \ldots, x_m)$, we obtain $Ax = \sum_{i=2}^{m} x_i A_i = \sum_{i=3}^{m} x_i (A_i - b_i A_2)$ and so

$$TAx \equiv \begin{pmatrix} 0 \\ * \\ k'_3 \\ \vdots \\ k'_m \end{pmatrix} \bmod p^{s-1}.$$

Then TAx and ${}^t(k'_1,\dots,k'_m) = T\,{}^t(k_1,\dots,k_m)$ are congruent modulo p^{s-1} except for first and second coordinates, and so Ax and ${}^t(k_1,\dots,k_m)$ are congruent modulo p^{s-1} except for α, β-th coordinates. Since the first coordinate of TAx is congruent to $0 \bmod p^{s-1}$, so is the α-th coordinate of Ax. This completes the proof. $\square$

LEMMA 6. *Let $\{v_1,\dots,v_m\}$ be a basis of M so that $(B(v_i, v_j))$ is reduced in the sense of Minkowski, and $\{w_1,\dots,w_m\}$ a basis of M given in Theorem. Defining a matrix $A = (a_{ij})$ in $GL_m(\mathbf{Z})$ by $(w_1,\dots,w_m) = (v_1,\dots,v_m)A$, we put*

$$S := \left\{ Af \mod p^s \;\middle|\; \begin{array}{l} {}^t f = (f_1, f_2,\dots,f_m),\ f_1 \equiv 0 \mod p^s, \\ f_2 \not\equiv 0 \mod p,\ f_3 \equiv \cdots \equiv f_m \equiv 0 \mod p \end{array} \right\}.$$

Choosing a coordinate α by the condition $a_{\alpha 2} \not\equiv 0 \bmod p$, there is a coordinate $\beta\,(\neq \alpha)$ which satisfies:

For an integral vector $h = {}^t(h_1,\dots,h_m) \in \mathbf{Z}^m$ with $h_\alpha \not\equiv 0 \bmod p$, there exists an element $r = {}^t(r_1,\dots,r_m) \in S$ so that

$$r_\alpha \equiv h_\alpha \mod p^s \text{ and } |r_i - h_i| \leq p/2 \quad \text{if} \quad i \neq \beta.$$

Proof. We take integers b_i $(1 \leq i \leq m)$ so that $a_{\alpha i} \equiv b_i a_{\alpha 2} \bmod p^{s-1}$. It is easy to see

$$S = \{f_2 A_2 + pAx \mod p^s \mid f_2 \not\equiv 0 \mod p,\ {}^t x = (0, x_2,\dots,x_m) \in \mathbf{Z}^m\},$$

where A_2 is the second column vector of A. We define an integer $f_2\,(\not\equiv 0 \bmod p)$ by $h_\alpha \equiv f_2 a_{\alpha 2} \bmod p^s$, and take integers $k_1,\dots,k_m$ so that $k_\alpha = 0$, and $|h_i - f_2 a_{i2} - pk_i| \leq p/2$ if $i \neq \alpha$. Applying Lemma 5, there is an integer $\beta\,(\neq \alpha)$ dependent only on A so that there is an integral vector $x = {}^t(x_1,\dots,x_m)$ with $x_1 = 0$ satisfying

$$g_i \equiv k_i \mod p^{s-1} \quad \text{for} \quad i \neq \beta,$$

putting ${}^t(g_1,\dots,g_m) := Ax$. Thus we have

$$(h - (f_2 A_2 + pAx))_i \equiv \begin{cases} 0 \mod p^s & \text{if } i = \alpha, \\ h_i - f_2 a_{i2} - pk_i \mod p^s & \text{if } i \neq \beta,\ \alpha. \end{cases}$$

Hence $r := f_2 A_2 + pAx$ is a required vector in S. $\square$

LEMMA 7. *Keep the situation in Lemma 6. Then we have*

$$a_{12} \not\equiv 0 \mod p \quad \textit{and} \quad a_{i2} \equiv 0 \mod p \quad \textit{for} \quad i > 1$$

https://doi.org/10.1017/S0027763000004773 Published online by Cambridge University Press

if (i) $m \geq 4$, (ii) $\min(M + \mathbf{Z}[p^{-s}w]) < \min(M)^{\kappa}$ *for every* $w = \sum_{i=2}^{m} f_i w_i \in M$ *with* $f_2 \not\equiv 0 \bmod p$ *and* $f_3 \equiv \cdots \equiv f_m \equiv 0 \bmod p$, *and* (iii) $\min(M)$ *is larger than some constant dependent on* m, κ *and* p.

Proof. We put $K := \min(M)^{\kappa}$. By making $\min(M)$ large so that

$$\frac{1}{4}\sqrt{Q(v_\alpha)/K} \geq \frac{1}{4}\min(M)^{(1-\kappa)/2} > p,$$

Lemma 6 yields that there is an integral vector $r = {}^t(r_1, \ldots, r_m) \in S$ so that $r_\alpha \equiv 1 \bmod p^s$ and $\frac{1}{4}\sqrt{Q(v_\alpha)/K} < r_i < \frac{1}{2}\sqrt{Q(v_\alpha)/K}$ for $i \neq \alpha, \beta$. Defining an element $w = \sum_{i=1}^{m} f_i w_i \in M$ by ${}^t(f_1, \ldots, f_m) = A^{-1}r$, $r \in S$ yields $f_1 \equiv 0 \bmod p^s$, $f_2 \not\equiv 0 \bmod p$, $f_3 \equiv \cdots \equiv f_m \equiv 0 \bmod p$, and then the assumption implies $\min(M + \mathbf{Z}[p^{-s}w]) < \min(M)^{\kappa} < c_1 \min(M)$ for a sufficiently large $\min(M)$, and then Lemma 4 implies that

$$\min(M + \mathbf{Z}[p^{-s}w]) \asymp \min_{\substack{b \in \mathbf{Z} \\ p^s \nmid b}} \Big(\sum_{i=1}^{m} \lceil b r_i p^{-s} \rceil^2 Q(v_i)\Big).$$

Hence, from the assumption $\min(M + \mathbf{Z}[p^{-s}w]) < \min(M)^{\kappa}$ follows

$$\min_{\substack{b \in \mathbf{Z} \\ p^s \nmid b}} \Big(\sum_{i=1}^{m} \lceil b r_i p^{-s} \rceil^2 Q(v_i)\Big) \ll \min(M)^{\kappa}.$$

Taking out α and γ-th coordinates for $\gamma \neq \alpha, \beta$, Lemma 1 gives

$$Q(v_\alpha) Q(v_\gamma) \ll \min(M)^{2\kappa} p^{2s},$$

which implies

$$\begin{aligned} Q(v_1)^2 Q(v_\alpha) Q(v_\gamma) &= (Q(v_1) Q(v_\alpha))(Q(v_1) Q(v_\gamma)) \\ &\ll (Q(v_\alpha) Q(v_\gamma))^2 \ll \min(M)^{4\kappa} p^{4s}. \end{aligned}$$

If $1 \notin \{\alpha, \gamma\}$, then it is easy to see, by the assumption on the basis $\{w_i\}$ in Theorem

$$Q(v_1) Q(v_\alpha) Q(v_\gamma) \asymp d\mathbf{Z}[v_1, v_\alpha, v_\gamma] \geq p^{4s}.$$

Hence the above two inequalities imply $Q(v_1) \ll \min(M)^{4\kappa} < \min(M)^{4/7}$. This is a contradiction if $\min(M)$ is sufficiently large. Thus we have $1 \in \{\alpha, \gamma\}$. By the assumption $m \geq 4$, there is a number γ' with $\gamma' \neq \alpha, \beta, \gamma$ and $1 \leq \gamma' \leq m$. Similarly we have $1 \in \{\alpha, \gamma'\}$ and so $\alpha = 1$. Since the number α is given only by the condition $a_{\alpha 2} \not\equiv 0 \mod p$, we have $a_{i2} \equiv 0 \mod p$ if $i \neq 1$. $\square$

Proof of Theorem in the case of $m \geq 4$.

We define bases $\{v_i\}$, $\{w_i\}$ of M, a matrix A and others as in Lemma 6. If there is an element $w = \sum_{i=2}^{m} f_i w_i \in M$ with $f_2 \not\equiv 0 \mod p$ and $f_3 \equiv \cdots \equiv f_m \equiv 0 \mod p$ such that the inequality (i) in Theorem is true, then there is nothing to do. Hence we may assume

$$\min(M + \mathbf{Z}[p^{-s}w]) < \min(M)^{\kappa}$$

for every $w = \sum_{i=2}^{m} f_i w_i$ with $f_2 \not\equiv 0 \mod p$ and $f_3 \equiv \cdots \equiv f_m \equiv 0 \mod p$. We will show that this leads us to a contradiction. Assuming that $\min(M)$ is sufficiently large, we have $\min(M)^{\kappa} < c_1 \min(M)$. Now Lemma 4 implies, for such a vector w

$$\min_{\substack{b \in \mathbf{Z} \\ p^s \nmid b}} \left(\sum_{i=1}^{m} \lceil b r_i p^{-s} \rceil^2 Q(v_i)\right) \asymp \min(M + \mathbf{Z}[p^{-s}w]) < \min(M)^{\kappa},$$

where ${}^t(r_1, \ldots, r_m) = A\,{}^t(0, f_2, \ldots, f_m)$. Now Lemma 7 implies

$$a_{12} \not\equiv 0 \mod p \quad \text{and} \quad a_{i2} \equiv 0 \mod p \quad \text{for} \quad i \geq 2.$$

We will show that $a_{ji} \not\equiv 0 \mod p$ implies $j \leq 2$ if $i \geq 3$. Take a natural number i with $3 \leq i \leq m$ and let f_i be an integer with $f_i \equiv 0 \mod p$. Then the above inequality implies, for ${}^t(r_1, \ldots, r_m) = A_2 + f_i A_i$

$$\begin{aligned} \min(M)^{\kappa} &\gg \min_{\substack{b \in \mathbf{Z} \\ p^s \nmid b}} \left(\sum_{j=1}^{m} \lceil b(a_{j2} + f_i a_{ji}) p^{-s} \rceil^2 Q(v_j)\right) \\ &\geqq \min_{\substack{b \in \mathbf{Z} \\ p^s \nmid b}} \left(\lceil b(a_{12} + f_i a_{1i}) p^{-s} \rceil^2 Q(v_1) + \lceil b(a_{j2} + f_i a_{ji}) p^{-s} \rceil^2 Q(v_j)\right) \end{aligned}$$

for every integer $j > 1$. Suppose that $a_{ji} \not\equiv 0 \mod p$ and $j \geq 3$. We will show a contradiction. Let us consider the equation in $x \in \mathbf{Z}$

$$a_{j2} + f_i a_{ji} \equiv (a_{12} + f_i a_{1i}) x \mod p^s.$$

It is equivalent to

$$f_i (a_{ji} - a_{1i} x) \equiv a_{12} x - a_{j2} \mod p^s.$$

We note $a_{j2} \equiv 0 \mod p$ and $a_{ji} \not\equiv 0 \mod p$. Hence the equation has a solution

https://doi.org/10.1017/S0027763000004773 Published online by Cambridge University Press

f_i ($\equiv 0 \mod p$) if $x \equiv 0 \mod p$. So we have, replacing $b(a_{12} + f_i a_{12})$ by b

$$\min(M)^{\kappa} \gg \min_{\substack{b \in \mathbf{Z} \\ p^s \nmid b}} (\lceil bp^{-s} \rceil^2 Q(v_1) + \lceil bxp^{-s} \rceil^2 Q(v_j))$$

for every integer x ($\equiv 0 \mod p$).

The inequality $\frac{1}{4}\sqrt{Q(v_1)/\min(M)^{\kappa}} \geq \frac{1}{4}\min(M)^{(1-\kappa)/2} > p$ and Lemma 2 imply

$$Q(v_1)Q(v_j) \ll \min(M)^{2\kappa} p^{2s}.$$

The assumption $j \geq 3$ and $d\mathbf{Z}[v_1, v_2, v_3] \equiv 0 \mod p^{4s}$ imply

$$\begin{aligned} Q(v_1)p^{4s} &\leq Q(v_1)d\mathbf{Z}[v_1, v_2, v_3] \ll Q(v_1)^2 Q(v_2)Q(v_3) \\ &\ll (Q(v_1)Q(v_j))^2 \ll \min(M)^{4\kappa} p^{4s} \end{aligned}$$

and hence $\min(M) \leq Q(v_1) \ll \min(M)^{4\kappa}$. Hence if $\min(M)$ is sufficiently large, this inequality does not hold. Thus we have shown $a_{ji} \equiv 0 \mod p$ if $i \geq 3$ and $j \geq 3$. Hence Lemma 7 yields

$$A \equiv \begin{pmatrix} * & * & * & \cdots & * \\ * & * & * & \cdots & * \\ * & 0 & 0 & \cdots & 0 \\ & & \cdots & & \\ * & 0 & 0 & \cdots & 0 \end{pmatrix} \mod p.$$

This contradicts $A \in GL_m(\mathbf{Z})$ if $m \geq 4$. Thus the theorem has been proved if $m \geq 4$. □

Next we must prove **the case of $m = 3$**. Let $\{v_i\}$, $\{w_i\}$, A, s and others be as above. Assume for every integer f ($\equiv 0 \mod p$)

$$\min(M + \mathbf{Z}[p^{-s}(w_2 + fw_3)]) < \min(M)^{\kappa}.$$

We will show that this leads us to a contradiction, making $\min(M)$ sufficiently large. For an integer $f \equiv 0 \mod p$, Lemma 4 yields

$$\min(M + \mathbf{Z}[p^{-s}(w_2 + fw_3)]) \asymp \min_{p^s \nmid b} (\sum_{i=1}^{3} \lceil br_i p^{-s} \rceil^2 Q(v_i))$$

for ${}^t(r_1, r_2, r_3) = A\,{}^t(0,1,f)$, if the left-hand side is less than $c_1 \min(M)$. Hence we have

$$\min_{p^s \nmid b} \left(\sum_{i=1}^{3} \lceil b r_i p^{-s} \rceil^2 Q(v_i)\right) < \min(M)^{\kappa}$$

for every integer $f\,(\equiv 0 \bmod p)$, assuming that $\min(M)$ is sufficiently large.

Putting $A = \begin{pmatrix} * & S_1 & T_1 \\ * & S_2 & T_2 \\ * & S_3 & T_3 \end{pmatrix}$, we have

$$r_i = S_i + fT_i.$$

LEMMA 8. *Put $d_{ij} = S_i T_j - S_j T_i$, and take any coordinates α, β such that $S_\alpha \not\equiv 0 \bmod p$ and $d_{\alpha,\beta} \not\equiv 0 \bmod p$. Denote by $\bar{a}$ an integer which satisfies $a\bar{a} \equiv 1 \bmod p^s$ if $a \not\equiv 0 \bmod p$. If $x \equiv \overline{S_\alpha} S_\beta \bmod p$ holds for an integer x, then there is an integer $f\,(\equiv 0 \bmod p)$ so that $r_\beta \equiv r_\alpha x \bmod p^s$. The condition $r_\beta \equiv r_\alpha x \bmod p^s$ implies for $\gamma \neq \alpha, \beta$*

$$r_\gamma \equiv r_\alpha \overline{d_{\alpha\beta}}(d_{\gamma\beta} + d_{\alpha\gamma}x) \bmod p^s.$$

Proof. Suppose $x \equiv \overline{S_\alpha} S_\beta \bmod p$. The equation $r_\beta \equiv r_\alpha x \bmod p^s$ is equivalent to

$$f(T_\beta - T_\alpha x) \equiv S_\alpha x - S_\beta \bmod p^s. \tag{6}$$

Substituting $x = \overline{S_\alpha} S_\beta + py$, it becomes

$$f(T_\beta - T_\alpha \overline{S_\alpha} S_\beta - pT_\alpha y) \equiv pS_\alpha y \bmod p^s$$

and so

$$f(d_{\alpha\beta} - pS_\alpha T_\alpha y) \equiv pS_\alpha^2 y \bmod p^s.$$

Since $d_{\alpha\beta} \not\equiv 0 \bmod p$, this is indeed soluble for $f\,(\equiv 0 \bmod p)$.
Supposing $r_\beta \equiv r_\alpha x \bmod p^s$, we have

$$\begin{aligned} d_{\gamma\beta} + d_{\alpha\gamma}x &\equiv S_\gamma T_\beta - S_\beta T_\gamma + (S_\alpha T_\gamma - S_\gamma T_\alpha)x \\ &\equiv (S_\alpha x - S_\beta)T_\gamma + S_\gamma(T_\beta - T_\alpha x) \equiv (T_\beta - T_\alpha x)(fT_\gamma + S_\gamma) \text{ by (6)} \\ &\equiv r_\gamma(T_\beta - T_\alpha x) \equiv r_\gamma \overline{r_\alpha}(r_\alpha T_\beta - T_\alpha r_\alpha x) \\ &\equiv r_\gamma \overline{r_\alpha}\{(S_\alpha + fT_\alpha)T_\beta - T_\alpha(S_\beta + fT_\beta)\} \equiv r_\gamma \overline{r_\alpha} d_{\alpha\beta} \bmod p^s, \end{aligned}$$

which yields $r_\gamma \equiv r_\alpha \overline{d_{\alpha\beta}}(d_{\gamma\beta} + d_{\alpha\gamma}x) \bmod p^s$, □

LEMMA 9. *We have*

https://doi.org/10.1017/S0027763000004773 Published online by Cambridge University Press

$$\min_{p^s \nmid b} (\lceil bp^{-s} \rceil^2 Q(v_\alpha) + \lceil bxp^{-s} \rceil^2 Q(v_\beta) + \lceil b\overline{d_{\alpha\beta}}(d_{\gamma\beta} + d_{\alpha\gamma}x)p^{-s} \rceil^2 Q(v_\gamma)) < \min(M)^\kappa \tag{7}$$

for every integer x $(\equiv \overline{S_\alpha} S_\beta \mod p)$.

Proof. This follows directly from Lemma 8, replacing b by $b\overline{r_\alpha}$. □

LEMMA 10. *If the constant* C *in Theorem is sufficiently large, then we have* $\{\alpha, \beta\} = \{1,2\}$ *and* $\gamma = 3$, *and* $S_3 \equiv T_3 \equiv 0 \mod p$ *and*

$$Q(v_1) Q(v_2) \leq 16 \min(M)^{2\kappa} p^{2s}. \tag{8}$$

Proof. Put $K := \min(M)^\kappa$. Since we may assume

$$\frac{1}{4}\sqrt{Q(v_\alpha)/K} \geq \frac{1}{4}\min(M)^{(1-\kappa)/2} > p,$$

applying Lemma 2 to the partial sum on α, β in (7), we have

$$Q(v_\alpha) Q(v_\beta) \leq 16K^2 p^{2s}.$$

If α or $\beta = 3$, then it implies

$$\begin{aligned} Q(v_1) dM &\ll (Q(v_1) Q(v_2))(Q(v_1) Q(v_3)) \ll (Q(v_\alpha) Q(v_\beta))^2 \\ &\leq 16^2 K^4 p^{4s}. \end{aligned}$$

Now $dM \geq p^{4s}$ yields $\min(M) \leq Q(v_1) \ll K^4 < \min(M)^{4/7}$. This is a contradiction if $\min(M)$ is larger than constant dependent on $m = 3$. Thus we have $\{\alpha, \beta\} = \{1,2\}$. Since α is taken under the condition $S_\alpha \not\equiv 0 \mod p$ only, we have $S_3 \equiv 0 \mod p$, and since β is taken under the condition $d_{\alpha\beta} \not\equiv 0 \mod p$, we have $d_{\alpha 3} = S_\alpha T_3 - S_3 T_\alpha \equiv 0 \mod p$, which yields $T_3 \equiv 0 \mod p$ by $S_3 \equiv 0 \mod p$ and $S_\alpha \not\equiv 0 \mod p$. □

LEMMA 11. *Let* e *be the least integer such that*

$$p^{e+1} \geq \frac{1}{4}\min(M)^{(1-\kappa)/2}. \tag{9}$$

Then we have

$$S_3 \equiv T_3 \equiv 0 \mod p^e.$$

Proof. Put $K := \min(M)^{\kappa}$. If $p^{1+\mathrm{ord}_p d_{\alpha 3}} < \frac{1}{4}\sqrt{\min(M)/K}$, then we have $p^{1+\mathrm{ord}_p d_{\alpha 3}} < \frac{1}{4}\sqrt{Q(v_\alpha)/K}$, and applying Lemma 2 to the partial sum on α, $\gamma\,(=3)$ in (7), we have

$$Q(v_\alpha)Q(v_3) \leq 16K^2p^{2s}.$$

This is the contradiction as in the proof of the previous lemma. Thus we have $p^{1+\mathrm{ord}_p d_{\alpha 3}} \geq \frac{1}{4}\sqrt{\min(M)/K}$ and hence $\mathrm{ord}_p d_{\alpha 3} \geq e$.

Let us see the inequality $\mathrm{ord}_p d_{\beta 3} \geq e$. If $S_\beta \not\equiv 0 \bmod p$, then replacing b by $b\bar{x}$ in (7), we get

$$\min_{p^s \nmid b} (\lceil bp^{-s}\rceil^2 Q(v_\beta) + \lceil \overline{d_{\alpha\beta}}(d_{3\beta}\bar{x} + d_{\alpha 3})p^{-s}\rceil^2 Q(v_3)) < K$$

for every integer $\bar{x} \equiv S_\alpha \overline{S_\beta} \bmod p$. Similarly to the case of α, we have the inequality $\mathrm{ord}_p d_{\beta 3} \geq e$.

Next suppose $S_\beta \equiv 0 \bmod p$. Then the inequality (7) holds for every integer $x \equiv 0 \bmod p$. Suppose that the minimum of the left-hand side is attained by b with $0 \neq |b| \leq p^s/2$ and $b \equiv 0 \bmod p^{s-1}$. Putting $b = Bp^{s-1}$, we have

$$K \geq \lceil Bp^{-1}\rceil^2 Q(v_\alpha) = B^2p^{-2}Q(v_\alpha) \geq p^{-2}Q(v_\alpha)$$

and so $\min(M) \leq Q(v_\alpha) < Kp^2 = p^2\min(M)^{\kappa}$, which is a contradiction if $\min(M)$ is sufficiently large. Thus the minimum is attained by an integer b with $b \not\equiv 0 \bmod p^{s-1}$ and so (7) implies

$$\min_{p^{s-1} \nmid b} (\lceil bxp^{-s}\rceil^2 Q(v_\beta) + \lceil b\overline{d_{\alpha\beta}}(d_{3\beta} + d_{\alpha 3}x)p^{-s}\rceil^2 Q(v_3)) < K$$

for every $x \equiv 0 \bmod p$. Letting $x = py$ with $y \not\equiv 0 \bmod p$ and replacing b by $b\bar{y}$, we have

$$\min_{p^{s-1} \nmid b} (\lceil bp^{1-s}\rceil^2 Q(v_\beta) + \lceil b\overline{d_{\alpha\beta}}(d_{3\beta}p^{-1}\bar{y} + d_{\alpha 3})p^{1-s}\rceil^2 Q(v_3)) < K$$

for every integer $\bar{y} \not\equiv 0 \bmod p$. Here we note $d_{3\beta} \equiv 0 \bmod p$ by $S_3 \equiv T_3 \equiv 0 \bmod p$. Hence if $p^{\mathrm{ord}_p(d_{3\beta})} \leq \frac{1}{4}\sqrt{Q(v_\beta)/K}$, then Lemma 2 implies

$$Q(v_\beta)Q(v_3) \leq 16K^2p^{2(s-1)}.$$

This is a contradiction as in the case of α. Hence we have $p^{\mathrm{ord}_p(d_{3\beta})} >$

https://doi.org/10.1017/S0027763000004773 Published online by Cambridge University Press

$\frac{1}{4}\sqrt{Q(v_\beta)/K} > \frac{1}{4}\sqrt{\min(M)/K}$ and so $\mathrm{ord}_p(d_{3\beta}) \geq e+1 > e$. Thus we have obtained $d_{3\alpha} \equiv d_{3\beta} \equiv 0 \mod p^e$, and so

$$S_3T_\alpha \equiv S_\alpha T_3 \mod p^e \text{ and } S_3T_\beta \equiv S_\beta T_3 \mod p^e.$$

Hence we have $S_3 d_{\alpha\beta} = S_3(S_\alpha T_\beta - S_\beta T_\alpha) \equiv S_\alpha S_\beta T_3 - S_\beta S_\alpha T_3 \equiv 0 \mod p^e$ and so $S_3 \equiv 0 \mod p^e$ and $T_3 \equiv \overline{S_\alpha} S_3 T_\alpha \mod p^e \equiv 0 \mod p^e$. $\square$

LEMMA 12. *Let f be the least integer such that $p^f > c_5 \min(M)^\kappa$, where c_5 is some absolute constant. Then we have*

$$d_{\alpha 3} \equiv 0 \mod p^{s-f-1}.$$

Proof. Put $K := \min(M)^\kappa$. Suppose that an integer b with $0 \neq |b| \leq p^s/2$ gives the minimum of the left-hand side of the equality (7).
Suppose $b(d_{3\beta} + d_{\alpha 3}x) \not\equiv 0 \mod p^s$; since $d_{3\beta} + d_{\alpha 3}x \equiv 0 \mod p^e$ by Lemma 11, the denominator of $b(d_{3\beta} + d_{\alpha 3}x)p^{-s}$ divides p^{s-e}. Thus the inequality (7) gives

$$K > \lceil b\overline{d_{\alpha\beta}}(d_{3\beta} + d_{\alpha 3}x)p^{-s}\rceil^2 Q(v_3) \geq p^{-2(s-e)}Q(v_3),$$

which implies $Q(v_3) < Kp^{2(s-e)}$. Thus the inequality (8) in Lemma 10 gives

$$\begin{aligned} p^{4s} &\leq dM \asymp Q(v_1)Q(v_2)Q(v_3) < 16K^3p^{4s-2e} \\ &\ll 16K^3p^{4s}\frac{16p^2}{\min(M)^{1-\kappa}} \quad \text{by (9)} \\ &= 16^2\min(M)^{4\kappa-1}p^{4s+2}. \end{aligned}$$

Thus we have $\min(M)^{1-4\kappa} \ll p^2$, and so making the constant C in Theorem larger, we have a contradiction. Hence we may assume that b runs over integers such that

$$(10) \qquad b(d_{3\beta} + d_{\alpha 3}x) \equiv 0 \mod p^s \text{ and } p^s \nmid b$$

in the left-hand side of the inequality (7). By $\frac{1}{4}\sqrt{Q(v_\alpha)/K} \geq \frac{1}{4}\min(M)^{(1-\kappa)/2} > 3p$ for a sufficiently large C, there is an integer y such that $y \equiv \overline{S_\alpha}S_\beta \mod p$ and

$$(11) \qquad \frac{1}{4}\sqrt{Q(v_\alpha)/K} < y < y+p < \frac{1}{2}\sqrt{Q(v_\alpha)/K}.$$

Put $x = y$ or $= y+p$, and suppose that an integer b with $0 \neq |b| \leq p^s/2$ gives the minimum of the left-hand side of the inequality (7). Then we have

https://doi.org/10.1017/S0027763000004773 Published online by Cambridge University Press

$$K > \lceil bp^{-s} \rceil^2 Q(v_\alpha) = b^2 p^{-2s} Q(v_\alpha),$$

which yields

$$| bxp^{-s} | < \sqrt{K/Q(v_\alpha)}\, p^s \cdot \frac{1}{2} \sqrt{Q(v_\alpha)/K} p^{-s} = 1/2.$$

Hence the inequality (7) gives

$$\begin{aligned} K &> \lceil bxp^{-s} \rceil^2 Q(v_\beta) = b^2 x^2 p^{-2s} Q(v_\beta) \\ &> b^2 \frac{Q(v_\alpha)}{16K} p^{-2s} Q(v_\beta) \quad \text{by (11)} \\ &= b^2 \frac{Q(v_\alpha) Q(v_\beta)}{16K} p^{-2s} \gg \frac{b^2}{16K}, \end{aligned}$$

where we used the inequality $Q(v_\alpha) Q(v_\beta) \asymp d\mathbf{Z}[v_\alpha, v_\beta] \geq p^{2s}$. Thus we have obtained $| b | < c_5 K$ for some absolute constant c_5. Then the way of choice of f implies $p^f > c_5 K > | b |$ and we have $f \geq \operatorname{ord}_p b$. The equality (10) implies

$$d_{3\beta} + d_{\alpha 3} x \equiv 0 \mod p^{s - \operatorname{ord}_p b} \equiv 0 \mod p^{s-f}.$$

Since this is true for $x = y$ and $= y + p$, we have $d_{\alpha 3} \equiv 0 \mod p^{s-f-1}$ □

LEMMA 13. *Let g be the least integer such that $p^g > c_6 \min(M)^\varkappa$, where c_6 is some absolute constant. Then we have*

$$d_{\beta 3} \equiv 0 \mod p^{s-g-1}.$$

Proof. Put $K := \min(M)^\varkappa$. Since α is determined only by the condition $S_\alpha \not\equiv 0 \mod p$, replacing α by β, we get the assertion from Lemma 12 if $S_\beta \not\equiv 0 \mod p$. Hence we may assume $S_\beta \equiv 0 \mod p$. So the inequality (7) holds for every integer x ($\equiv 0 \mod p$). Letting $x = py$ with $y \not\equiv 0 \mod p$ and replacing b by $b\bar{y}$, we have, replacing $\bar{y}$ by y again

$$\text{(12)} \quad \min_{p^s \nmid b} (\lceil byp^{-s} \rceil^2 Q(v_\alpha) + \lceil bp^{1-s} \rceil^2 Q(v_\beta) + \lceil b\overline{d_{\alpha\beta}}(d_{3\beta} y + d_{\alpha 3} p) p^{-s} \rceil^2 Q(v_3)) < K$$

for every integer y ($\not\equiv 0 \mod p$). If the minimum of the left-hand side is given by an integer b with $0 \neq | b | \leq p^s/2$ and $b \equiv 0 \mod p^{s-1}$, then we have

$$K > Q(v_\alpha)/p^2,$$

noting that the denominator of byp^{-s} is equal to p. It implies $Kp^2 > Q(v_\alpha) \geq$

https://doi.org/10.1017/S0027763000004773 Published online by Cambridge University Press

$\min(M)$ and so $\min(M)^{1-\varkappa} < p^2$, which is a contradiction if C is a sufficiently large number. Thus the minimum of the left-hand side of (12) is attained by $b \not\equiv 0 \bmod p^{s-1}$. Let an integer b with $0 \neq |b| \leq p^s/2$ give the minimum of the left-hand side of (12) and put

$$b = a_1 + a_2 p^{s-1} \text{ with } 0 \neq |a_1| \leq p^{s-1}/2.$$

Now we claim both $a_2 = 0$ and $|by| < p^{s-1}/2$ if $\sqrt{K/Q(v_\beta)}\,|y| \leq 1/2$.
First, let us see

$$(13) \qquad |a_2| \leq p/2.$$

If p is odd, then we have

$$\begin{aligned} |a_2| &= |a_1 - b|/p^{s-1} \leq (|a_1| + |b|)/p^{s-1} \\ &\leq ((p^{s-1} - 1)/2 + (p^s - 1)/2)/p^{s-1} = p/2 + 1/2 - p^{-(s-1)} \end{aligned}$$

and by virtue of the integrality of a_2, we have $|a_2| \leq p/2$. If $p = 2$, then we have

$$|a_2| \leq (|a_1| + |b|)/2^{s-1} \leq (2^{s-2} + 2^{s-1})/2^{s-1} = 3/2,$$

and hence $|a_2| \leq 1 = p/2$.
Next, we put

$$by \equiv a_1 y + a_2' p^{s-1} \bmod p^s$$

with $a_2' \equiv a_2 y \bmod p$ and $|a_2'| \leq p/2$. Then we will see that

$$(14) \qquad |a_1 y| < p^{s-1}/2 \quad \text{and} \quad |a_1 y + a_2' p^{s-1}| \leq p^s/2,$$

taking a_2' with $(a_1 y) a_2' \leq 0$ if $p = 2$. The inequality (12) implies

$$K > \lceil b p^{1-s} \rceil^2 Q(v_\beta) = (a_1 p^{1-s})^2 Q(v_\beta)$$

and so $|a_1| < \sqrt{K/Q(v_\beta)}\, p^{s-1}$, which yields $|a_1 y| < p^{s-1}/2$ if $\sqrt{K/Q(v_\beta)}\,|y| \leq 1/2$. Hence we have, for $p \neq 2$

$$|a_1 y + a_2' p^{s-1}| < p^{s-1}/2 + \frac{p-1}{2} p^{s-1} = p^s/2.$$

If $p = 2$ and $a_2' \neq 0$, then we have $|a_1 y + a_2' 2^{s-1}| = 2^{s-1} - |a_1 y| \leq 2^{s-1}$. If $p = 2$ and $a_2' = 0$, then $|a_1 y| < 2^{s-1}$ is clear. Thus the inequalities in (14) have been shown, and then the inequalities (12) and (14) yield

$$K > \lceil b y p^{-s} \rceil^2 Q(v_\alpha) = (a_1 y + a_2' p^{s-1})^2 p^{-2s} Q(v_\alpha)$$

and hence

(15) $$|a_1y + a_2'p^{s-1}| \le \sqrt{K/Q(v_\alpha)}\, p^s.$$

Suppose $a_2 \ne 0$; then we have $a_2 \not\equiv 0 \mod p$ by (13) and so $a_2' \ne 0$. Thus the left-hand side of (15) is larger than

$$p^{s-1} - |a_1y| > p^{s-1} - p^{s-1}/2 = p^{s-1}/2,$$

and hence we have $p^{s-1}/2 < \sqrt{K/Q(v_\alpha)}\, p^s \le \min(M)^{(\varkappa-1)/2} p^s$, which yield the contradiction $\min(M)^{(1-\varkappa)/2} < 2p$. Thus we have shown the claim $a_2 = 0$ and $b = a_1$, that is, an integer b which gives the minimum of the left-hand side of (12), satisfies two inequalities

$$|by| < p^{s-1}/2 \quad \text{and} \quad 0 \ne |b| \le p^{s-1}/2 \quad \text{if} \quad \sqrt{K/Q(v_\beta)}\,|y| \le 1/2.$$

Because of $\frac{1}{4}\sqrt{Q(v_\beta)/K} \ge \frac{1}{4}\min(M)^{(1-\varkappa)/2} \ge p$, we can take $y \not\equiv 0 \mod p$ so that

$$\frac{1}{4}\sqrt{Q(v_\beta)/K} < |y| < \frac{1}{2}\sqrt{Q(v_\beta)/K},$$

then letting an integer b with $0 \ne |b| \le p^s/2$ give the minimum of the left-hand side of (12), we have $|b| \le p^{s-1}/2$ and then the inequality (12) and the above claim $|by| < p^{s-1}/2$ imply

$$K > \lceil byp^{-s} \rceil^2 Q(v_\alpha) = b^2y^2p^{-2s}Q(v_\alpha) \ge b^2\frac{Q(v_\alpha)Q(v_\beta)}{16K}p^{-2s}$$
$$\gg b^2/K \quad \text{because of} \quad Q(v_\alpha)Q(v_\beta) \gg p^{2s}.$$

Thus we have

$$|b| < c_6K \quad \text{if} \quad \frac{1}{4}\sqrt{Q(v_\beta)/K} < |y| < \frac{1}{2}\sqrt{Q(v_\beta)/K}$$

where c_6 is an absolute constant. Now we take the least integer g so that $p^g > c_6K$, which implies $|b| < p^g$. Taking an integer z so that $\frac{1}{4}\sqrt{Q(v_\beta)/K} < z < z + p < \frac{1}{2}\sqrt{Q(v_\beta)/K}$, we put $y = z$ or $= z + p$, and let b give the minimum of the left-hand side of (12). Suppose $b(d_{3\beta}y + d_{\alpha 3}p) \not\equiv 0 \mod p^s$; then the denominator of $b\overline{d_{\alpha\beta}}(d_{3\beta}y + d_{\alpha 3}p)p^{-s}$ is at most p^{s-e} for the integer e in Lemma 11. Hence the inequality (12) implies $K > p^{-2(s-e)}Q(v_3)$ and hence a contradiction as in the proof of Lemma 12. Therefore we have $b(d_{3\beta}y + d_{\alpha 3}p) \equiv 0 \mod p^s$. Noting $|b| < p^g$ as above, we have $d_{3\beta}y + d_{\alpha 3}p \equiv 0 \bmod p^{s-g}$ for $y = z$ or $= z + p$. Thus we have $d_{3\beta}p \equiv 0 \bmod p^{s-g}$ and so $\mathrm{ord}_p d_{3\beta} \geq s - g - 1$. □

Combining Lemma 12 with Lemma 13, we have

LEMMA 14. *There is an absolute constant c_7 so that*

$$d_{13} \equiv d_{23} \equiv 0 \bmod p^{s-h-1},$$

where h is the least integer so that $p^h > c_7 \min(M)^{\kappa}$.

LEMMA 15. *The inequality $g < s$ and $d_{13} \equiv d_{23} \equiv 0 \bmod p^g$ imply $p^g \leq 2\min(M)^{\kappa/2}p^{s/2}$.*

Proof. We recall

$$A = \begin{pmatrix} * & S_1 & T_1 \\ * & S_2 & T_2 \\ * & S_3 & T_3 \end{pmatrix}, \; d_{ij} = S_iT_j - S_jT_i, \; (B(w_i, w_j)) = (B(v_i, v_j))[A].$$

Hence we have

$$\begin{aligned} (B(v_i, v_j)) &= (B(w_i, w_j))[A^{-1}] \\ &\equiv \mathrm{diag}(\varepsilon, 0, 0)[A^{-1}] \bmod p^g \\ &\equiv \mathrm{diag}(\varepsilon, 0, 0)\left[\begin{pmatrix} 0 & 0 & * \\ * & * & * \\ * & * & * \end{pmatrix}\right] \text{ by } d_{13} \equiv d_{23} \equiv 0 \bmod p^g \\ &\equiv \begin{pmatrix} 0 & * & * \\ 0 & * & * \\ * & * & * \end{pmatrix}\begin{pmatrix} 0 & 0 & * \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \equiv \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & * \end{pmatrix} \bmod p^g. \end{aligned}$$

Since $(B(w_i, w_j)) \not\equiv 0 \bmod p$ and hence $(B(v_i, v_j)) \not\equiv 0 \bmod p$ by the assumption $s(M_p) = \mathbf{Z}_p$, we have $Q(v_3) \not\equiv 0 \bmod p$. For $i = 1$ or 2, we put $Q(v_i) = ap^g$, $B(v_i, v_3) = bp^g$ $(a, b \in \mathbf{Z})$, which imply $ap^gQ(v_3) - b^2p^{2g} = d\mathbf{Z}[v_i, v_3] \equiv 0 \bmod p^{2s}$. Therefore $s > g$ implies $a \equiv 0 \bmod p^g$, and so $Q(v_i) \equiv 0 \bmod p^{2g}$. Thus $s > g$ yields $Q(v_1) \equiv Q(v_2) \equiv 0 \bmod p^{2g}$, and hence $p^{4g} \leq Q(v_1)Q(v_2) \leq 16\min(M)^{2\kappa}p^{2s}$ by (8). □

Now let us complete the proof of Theorem in the case of $m = 3$. If we put $g = s - h - 1$ $(< s)$ for the number h in Lemma 14, we have $p^{s-h-1} \leq 2\min(M)^{\kappa/2}p^{s/2}$, and hence

$$p^{s/2} \leq 2 \min(M)^{\kappa/2} p^{h+1} < 2c_7 \min(M)^{3\kappa/2} p^2$$

by virtue of $p^{h-1} \leq c_7 \min(M)^{\kappa} < p^h$. Putting $\tilde{M} := M + \mathbf{Z}[p^{-s} w_2]$, $\tilde{M}$ satisfies the conditions (ii) and (iii). $[\tilde{M} : M] = p^s$ yields $\min(p^s \tilde{M}) \geq \min(M)$ and hence we have

$$\begin{aligned} \min(\tilde{M}) &\geq p^{-2s} \min(M) > 2^{-4} c_7^{-4} \min(M)^{1-6\kappa} p^{-8} \\ &\geq 2^{-4} c_7^{-4} p^{-8} \min(M)^{1-7\kappa} \cdot \min(M)^{\kappa}. \end{aligned}$$

Thus, if we take a sufficiently large number C which depends on p, c_7, we have $\min(\tilde{M}) \geq \min(M)^{\kappa}$. This contradicts our assumption. Thus we have completed the proof in the case of $m = 3$. □

§2

In this section we show that the assertion $\mathrm{R}_{m,2m+1}(N)$ is true if $m \geq 3$.

THEOREM. *Let m be a natural number ≥ 3, and N a lattice on a positive definite quadratic space W over $\mathbf{Q}$ with $\dim W = 2m + 1$. Let M be a lattice on a positive definite quadratic space V over $\mathbf{Q}$ with $\dim V = m$ and suppose that M_p is represented by N_p for every prime p. Let C_1 be a positive number. Then there is a positive number C_2 dependent only on C_1 and N so that if $\min(M) > C_2$, then there is a lattice M' on V so that*

(i) *M' contains M,*

(ii) *M'_p is primitively represented by N_p for every prime p,*

(iii) *$\min(M') > C_1$.*

Remark. In the case of $m = 2$, Theorem is false.

The following is immediate.

COROLLARY. *The assertion $\mathrm{APW}_{m,2m+1}(N)$ yields the assertion $\mathrm{A}_{m,2m+1}(N)$ if $m \geq 3$.*

The proof of the theorem is divided into several steps. Let M, N be lattices in Theorem. We may assume that $n(N) \subset 2\mathbf{Z}$ without loss of generality. Put

$$S := \{p \mid p \text{ is a prime which divides } 2dN\}.$$

LEMMA 1. *If a prime p is not in S, then M_p is primitively represented by N_p.*

Proof. Since p is odd and N_p is unimodular, N_p is isometric to

$$\perp_m \langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \rangle \perp \langle dN \rangle$$

and so M_p is primitively represented by N_p by Proposition 5.3.2 in [5]. □

LEMMA 2. *If a prime p in S and $\mathrm{ind} W_p = m$, then there is a constant $c_p(N)$ dependent only on N_p so that there exists a lattice $\tilde{M}_p$ on V_p which satisfies*
(i) $\tilde{M}_p \supset M_p$ and $[\tilde{M}_p : M_p] < c_p(N)$,
(ii) $\tilde{M}_p$ is primitively represented by N_p.

Proof. Let K be a submodule of N_p which is isometric to M_p; then by Lemma 3 in [3], there exists a submodule L of N_p so that $L \cong K$ and $[N_p \cap \mathbf{Q}_p L : L] < c_p(N)$ for a constant $c_p(N)$ dependent only on N_p. By virtue of $L \cong K \cong M_p$, there is an isometry σ from M_p to L, and then we have only to put $\tilde{M}_p = \sigma^{-1}(N_p \cap \mathbf{Q}_p L)$. □

LEMMA 3. *Let p be a prime. There exist two constants $r_p(N)$, $c_p(N)$ so that there exists a lattice $\tilde{M}$ ($\supset M$) on V which satisfies*
(i) $[\tilde{M} : M]$ is a power of the prime p,
(ii) $\tilde{M}_q$ is represented by N_q for every prime q,
(iii) $\mathrm{ord}_p s(\tilde{M}) < r_p(N)$,
(iv) $\min(\tilde{M}) > c_p(N) p^{t/2} \min(T_0)$, where a positive definite matrix T_0 is defined by $M = \langle p^t T_0 \rangle$ with $n(T_0)\mathbf{Z}_p = 2\mathbf{Z}_p$ by identifying the corresponding matrix and a lattice.

Proof. Let N_p' be a $2p^r\mathbf{Z}_p$-maximal lattice in N_p and we assume that r is the least positive integer. r is determined by N_p.
Suppose $\mathrm{ord}_p s(M_p) \geq r + 13$. Write

$$M = \langle p^{r+10+2a+c} T_0 \rangle,$$

where T_0 satisfies $n(T_0)\mathbf{Z}_p = 2\mathbf{Z}_p$ and $a \geq 1$, $c = 0$ or 1. Putting $b := 5 + a$, we have $p^b \geq 2^6 > 36$ and then Lemma 2 in [4] implies the existence of a positive constant $c(m, p)$ dependent only on m and p, and a matrix $H \in M_m(\mathbf{Z})$ so that $\det H$ is a power of p, $\min(p^{2b+c} T_0[H^{-1}]) > c(m, p) p^{b+c} \min(T_0)$, $p^{2b+c} T_0[H^{-1}] \not\equiv 0 \bmod p^5$ and finally $n(p^{2b+c} T_0[H^{-1}]) \subset 2\mathbf{Z}$. Hence there exists a lattice $\tilde{M}$

$(\supset M)$ such that $[\tilde{M}:M]$ is a power of p, $s(\tilde{M})\mathbf{Z}_p \supset p^{r+4}\mathbf{Z}_p$, $\min(\tilde{M}) > c(m,p)\, p^{r+b+c} \min(T_0) \geq c(m,p) p^{t/2} \min(T_0)$ and finally $n(\tilde{M}) \subset 2p^r\mathbf{Z}$. Thus the assertion (i) is clearly satisfied and then for every prime $q \neq p$, $\tilde{M}_q = M_q$ is represented by N_q. Since $n(\tilde{M})\mathbf{Z}_p \subset 2p^r\mathbf{Z}_p$, and $\mathbf{Q}_p\tilde{M} = \mathbf{Q}_pM$ is represented by $\mathbf{Q}_pN$ and moreover N_p' $(\subset \mathbf{Q}_pN)$ is a $2p^r\mathbf{Z}_p$-maximal lattice, $\tilde{M}_p$ is represented by N_p' and hence by N_p. Thus the assertion (ii) is satisfied. The assertion (iii) is satisfied for $r_p(N) = r + 13$. (iv) is satisfied for $c_p(N) := c(m,p)$.

Next suppose $\mathrm{ord}_p s(M_p) < r + 13$; then putting $\tilde{M} := M$, the assertions (i), ..., (iv) are satisfied if $r_p(N) = r + 13$, $c_p(N) = 1$.
Thus the assertion are true for $r_p(N) := r + 13$ and $c_p(N) := \min\{1, c(m,p)\}$. □

LEMMA 4. *There is a lattice $\tilde{M}$ $(\supset M)$ on V which satisfies*
(i) *any prime number dividing $[\tilde{M}:M]$ is in S,*
(ii) *there is a constant $c(N)$ depending only on N such that*

$$\min(\tilde{M}) > c(N) \min(M)^{1/2},$$

(iii) *$\tilde{M}_p$ is primitively represented by N_p if $p \notin S$, or if both $p \in S$ and $\mathrm{ind}\, W_p = m$,*
(iv) *if $p \in S$ and $\mathrm{ind}\, W_p = m - 1$, then there is a number $r_p(N)$ dependent only on N_p such that $\mathrm{ord}_p s(\tilde{M}_p) < r_p(N)$ and $\tilde{M}_p$ is represented by N_p.*

Proof. By Lemma 1, M_p is primitively represented by N_p if $p \notin S$. Using Lemma 2 if $p \in S$ and $\mathrm{ind}\, W_p = m$ and using Lemma 3 if $p \in S$ and $\mathrm{ind}\, W_p = m - 1$, we have only to enlarge M. □

SUBLEMMA. *Let $0 < k \leq m \leq n$ be integers and N_p, K_1 regular quadratic lattices over $\mathbf{Z}_p$ with $\mathrm{rank}\, N_p = n$, $\mathrm{rank}\, K_1 = k$. Moreover we assume that there is a quadratic space U over $\mathbf{Q}_p$ such that $\mathbf{Q}_pN_p \cong \mathbf{Q}_pK_1 \perp U$ and $\mathrm{ind}\, U \geq m - k$. Then there exists a constant $c = c(N_p, K_1, m, k)$ such that if $K = K_1 \perp K_2$ is a regular quadratic lattice of $\mathrm{rank}\, K = m$ and K is represented by N_p, then there is a submodule $K_0 \subset N_p$, which is isometric to K with $[N_p \cap \mathbf{Q}_pK_0 : K_0] < c$.*

Proof. This is nothing but Theorem 2 in [3] (r, n, m and M there, are replaced by k, m, n and N respectively). □

LEMMA 5. *Let p be a prime. Assume that there is a decomposition $M_p = M_{p,1} \perp M_{p,2}$ with $\mathrm{rank}\, M_{p,1} > 1$, then there is an isometry $\sigma : M_p \to N_p$ such that $[\mathbf{Q}_p\sigma(M_p) \cap N_p : \sigma(M_p)] < c_p(M_{p,1}, N_p)$, where $c_p(M_{p,1}, N_p)$ depends only on $M_{p,1}$*

and N_p.

Proof. Put $k = \operatorname{rank} M_{p,1}$. By virtue of the sublemma, we have only to show $\operatorname{ind} U \geq m - k$ where U is determined by $W_p \cong \mathbf{Q}_p M_{p,1} \perp U$. We know

$$\dim U = 2m + 1 - k = 2(m - k) + k + 1 \geq 2(m - k) + 3.$$

If, hence the inequality $\operatorname{ind} U < m - k$ holds, then we have

$$\dim U \leq 2 \operatorname{ind} U + 4 \leq 2(m - k - 1) + 4 = 2(m - k) + 2.$$

which contradicts $\dim U \geq 2(m - k) + 3$. Thus we have $\operatorname{ind} U \geq m - k$. □

Proof of Theorem.

By virtue of Lemma 4, we may suppose

(i) M_p is primitively represented by N_p if $p \notin S$ or if $p \in S$ and $\operatorname{ind} W_p = m$,

(ii) $\operatorname{ord}_p s(M_p) < r_p(N)$ if $p \in S$ and $\operatorname{ind} W_p = m - 1$, where $r_p(N)$ is only dependent on p and N_p,

(iii) $\min(M)$ is sufficiently large.

We are assuming that $n(N) \subset 2\mathbf{Z}$ and M_p is locally represented by N_p. So we have $n(M) \subset 2\mathbf{Z}$. Let a prime $p \in S$ satisfy $\operatorname{ind} W_p = m - 1$, and put $t_p := \operatorname{ord}_p s(M_p)$. By the assumption (ii), we have $0 \leq t_p \leq r_p(N)$. Let

$$X := \{x \in N_p \mid \operatorname{ord}_p Q(x) \leq r_p(N)\}.$$

The orthogonal group $O(N_p)$ and $\mathbf{Z}_p^\times$ act on X and the number of orbits is finite. Denote the set of representatives of orbits by $\tilde{X}$. Hence $\tilde{X}$ is a finite set and if $\operatorname{ord}_p Q(x) < r_p(N)$ for $x \in N_p$, then there exist an isometry $\sigma \in O(N_p)$ and $\varepsilon \in \mathbf{Z}_p^\times$ such that $\varepsilon\sigma(x) \in \tilde{X}$. For $x \in \tilde{X}$, we take a maximal lattice N_x ($\subset x^\perp$ in N_p), and put the norm $n(N_x) = p^{n_p(x)}\mathbf{Z}_p$. We take N_x so that $n_p(x)$ is minimal, and put

$$n_p = \max_{x \in \tilde{X}} n_p(x).$$

n_p is determined by $r_p(N)$, and hence only by N_p.

Let $M_p = J_1 \perp \cdots \perp J_a$ be a Jordan decomposition, where J_i is $p^{b_i}\mathbf{Z}_p$-modular and $0 \leq b_1 < b_2 < \cdots < b_a$. By virtue of $s(M_p) = s(J_1)$, we have $0 \leq b_1 = t_p < r_p(N)$. If $\operatorname{rank}(J_1) > 1$, then noting that the number of possiblities of isometry classes of J_1 is bounded by a number dependent only on $r_p(N)$ and $m = (\operatorname{rank} N - 1)/2$, Lemma 5 implies the existence of a lattice M' such that $[M' : M] < c_p(N_p)$ and M'_p is primitively represented by N_p, where $c_p(N_p)$ depends only on N_p. $[M' : M]M' \subset M$ implies $[M' : M]^2 \min(M') \geq \min(M)$ and hence

$\min(M') \geq [M' : M]^{-2} \min(M) > c_p(N_p)^{-2} \min(M)$. Since $c_p(N_p)$ depends only on N_p, $\min(M')$ is still large if $\min(M)$ is sufficiently large. Next, we assume $\operatorname{rank}(J_1) = 1$. If $b_2 = \operatorname{ord}_p s(J_2) \leq n_p$ holds, then applying Lemma 5 to $M_{p,1} := J_1 \perp J_2$, we can get the similar result. So we may assume

$$\operatorname{rank}(J_1) = 1 \quad \text{and} \quad b_2 > n_p.$$

Now we take a basis $\{w_1, \ldots, w_m\}$ of M so that the matrix $(B(w_i, w_j))$ satisfies the congruence condition in Theorem in §1, making it sufficiently close to bases of $J_1, \ldots, J_a$. Put $z_1 := w_1$, $z_i := w_i - B(w_1, w_i) Q(w_1)^{-1} w_1$ $(i \geq 2)$; then we have $M_p = \mathbf{Z}_p[w_1] \perp \mathbf{Z}_p[z_2, \ldots, z_m]$. Put $s := [(\operatorname{ord}_p Q(w_2) - \operatorname{ord}_p Q(w_1))/2]$; by applying Theorem in §1 to the scaling of M_p by $p^{-\operatorname{ord}_p Q(w_1)} = p^{-t_p}$, there exists an element $w \in \mathbf{Z}[w_2, \ldots, w_m] (\subset M)$ such that

$$\min(M + p^{-s}\mathbf{Z}[w]) > \min(M)^{1/8}, \; s(M + p^{-s}\mathbf{Z}[w]) \subset p^{t_p}\mathbf{Z},$$
$$\operatorname{ord}_p(d\mathbf{Z}[w_1, p^{-s}w]) \leq 2 + t_p.$$

Now we put

$$\tilde{M} := M + p^{-s+n_p}\mathbf{Z}[w].$$

Then we have

$$\tilde{M} \subset M + p^{-s}\mathbf{Z}[w],$$
$$\min(\tilde{M}) \geq \min(M + p^{-s}\mathbf{Z}[w]) > \min(M)^{1/8},$$
$$\operatorname{ord}_p d\mathbf{Z}[w_1, p^{-s+n_p}w] \leq 2 + t_p + 2n_p \leq 2 + r_p(N_p) + 2n_p,$$

and $\mathbf{Z}[w_1, p^{-s+n_p}w] \subset \tilde{M}$ is clear. Hence if $\tilde{M}_p$ is represented by N_p, there is a lattice $M' \supset \tilde{M}$ by Lemma 5 such that M'_p is primitively represented by N_p and $[M' : \tilde{M}]$ is bounded by a number dependent only on N_p, and it completes the proof of the theorem. Since $B(w, w_1)$ is sufficiently close to 0, we have

$$\begin{aligned}\tilde{M}_p &= \mathbf{Z}_p[z_1, \ldots, z_m] + p^{-s+n_p}\mathbf{Z}_p[w - B(w, w_1) Q(w_1)^{-1} w_1] \\ &= \mathbf{Z}_p[z_1] \perp (\mathbf{Z}_p[z_2, \ldots, z_m] + p^{-s+n_p}\mathbf{Z}_p[w - B(w, w_1) Q(w_1)^{-1} w_1]).\end{aligned}$$

Moreover we know that $\operatorname{ord}_p Q(z_1) = \operatorname{ord}_p Q(w_1) = t_p < r_p(N)$ and M_p is represented by N_p, and hence there is an isometry σ from M_p to N_p so that $\sigma(z_1) = \varepsilon x$ for $\varepsilon \in \mathbf{Z}_p^\times$ and $x \in \tilde{X}$.

Now $\operatorname{ord}_p s(w_1^\perp) = b_2 > n_p$ implies $s(\mathbf{Z}_p[z_2, \ldots, z_m]) \subset p^{n_p}\mathbf{Z}_p$ and $s(M_p + p^{-s}\mathbf{Z}_p[w]) \subset p^{t_p}\mathbf{Z}_p$ implies

$$B(\mathbf{Z}_p[z_2, \ldots, z_m], p^{-s+n_p}(w - B(w, w_1) Q(w_1)^{-1} w_1)) \subset p^{n_p+t_p}\mathbf{Z}_p.$$

https://doi.org/10.1017/S0027763000004773 Published online by Cambridge University Press

Finally we have $Q(p^{-s+n_p}(w-B(w,w_1)Q(w_1)^{-1}w_1))\in p^{2n_p+t_p}\mathbf{Z}_p$, since $B(w,w_1)$ is sufficiently close to 0 and $Q(p^{-s}w)\equiv 0 \bmod p^{t_p}$ and hence we have

$$s(\mathbf{Z}_p[z_2,\ldots,z_m]+p^{-s+n_p}\mathbf{Z}_p[w-B(w,w_1)Q(w_1)^{-1}w_1])\subset p^{n_p}\mathbf{Z}_p.$$

Hence $z_1^{\perp}$ in $\tilde{M}_p$ is represented by the maximal lattice N_x ($\subset x^{\perp}$ in N_p) of $\mathrm{ord}_p n(N_x)\le n_p$ because of $\mathbf{Q}_p(z_1^{\perp}$ in $\tilde{M}_p)\hookrightarrow \mathbf{Q}_p x^{\perp}$ and $\mathrm{ord}_p n(z_1^{\perp}$ in $\tilde{M}_p)\ge n_p$. Thus $\tilde{M}_p$ is represented by N_p, and hence we have completed the proof of the theorem. $\square$

§3

Let us see the behavior of the expected main term of the number of isometries from M to N when $n=2m+1$. The expected main term (= Siegel's weighted sum) is given by

$$c_m(dN)^{-m/2}(dM)^{m/2}\prod_p \alpha_p(M_p,N_p)$$

where c_m is a number independent of M and N, and $\alpha_p(M_p,N_p)$ is the local density. If a prime p is odd and both M_p and N_p are unimodular, then we know

$$\alpha_p(M_p,N_p)=\prod_{\substack{m+1\le e\le 2m\\ 2\mid e}}(1-p^{-e})\times\begin{cases}1+\chi_p(-dNdM)p^{-(m+1)/2} & \text{if } 2\nmid m\\ 1 & \text{if } 2\mid m,\end{cases}$$

where χ_p is the quadratic residue symbol. If we assume that $m>1$ and M_p is primitively represented by N_p for every prime p, then

$$\prod_p \alpha_p(M_p,N_p)>c(N)\prod_p(1+\varepsilon_p p^{-1})$$

where primes p in the left-hand side run all over the primes, and primes p in the right-hand side run over the set

$$\{p\mid p\neq 2 \text{ and } N_p \text{ is unimodular but } M_p \text{ is not so}\},$$

and $\varepsilon_p=0$ or $=\pm 1$ and the number $c(N)$ is only dependent on N. ε_p is defined as follows: When M_p/pM_p is isometric to R of dimension 1 and the radical over $\mathbf{Z}/p\mathbf{Z}$, ε_p is by definition $\chi_p(dRd(N_p/pN_p))$, where d denotes the discriminant and χ_p is the quadratic residue symbol. Otherwise we put $\varepsilon_p=0$. The right-hand side can tend to the zero when M varies. Note that there is a constant c such that

$$\prod_{p\mid t}(1-p^{-1})>c(\log\log t)^{-1}.$$

If we do not assume the existence of the primitive representation of M_p by N_p, then $\alpha_p(M_p, N_p)$ can tend to the zero for a single prime p when M varies. It is known (Corollary on p. 448 in [3]) that there is a constant $c(M_p, N_p)$ so that

$$\alpha_p(p^t M_p, N_p) > c(M_p, N_p)\begin{cases} 1 & \text{if } \operatorname{ind} W_p = m, \\ p^{-t} & \text{if } \operatorname{ind} W_p = m-1. \end{cases}$$

In our case, i.e. rank $N_p = 2$ rank $M_p + 1$, we have

$$\alpha_p(M_p, N_p) \geq [M_p' : M_p]^{-m} d_p(M_p', N_p)$$

for any lattice M_p' which contains M_p and is primitively represented by N_p, where $d_p(M_p', N_p)$ denotes the primitive density. We expect $[M_p' : M_p] \ll p^{(a_1+a_2)/2}$, where p^{a_i} denotes the i-th elementary divisor of the matrix corresponding to M_p. When we are concerned with the asymptotic formula of the number of isometries from M to N, we need a stronger estimate for error terms than in the primitive representation case.

On the contrary, from the arithmetic view-point, the primitive representation problem $\mathrm{APW}_{m,2m+1}$ yields automatically the representation problem $\mathrm{A}_{m,2m+1}$ by virtue of the validity of $\mathrm{R}_{m,2m+1}(N)$.

Appendix

PROPOSITION. *Let M be a lattice on a positive definite quadratic space over $\mathbf{Q}$ of* $\dim V = m$. *Let M_i $(i = 0, \ldots, r)$ be a lattice containing M on V, and let $x_i \in M_i$ give the minimum of M_i, i.e. $Q(x_i) = \min(M_i)$ and suppose that a module $K := \mathbf{Z}[x_1, \ldots, x_r]$ is of* rank r *and $x_0 \in \mathbf{Q}K$. Then we have*

$$\prod_{i=0}^{r} \min(M_i) \geq d(K + \mathbf{Z}[x_0])[\mathbf{Z}[x_0] \cap M : \mathbf{Z}[x_0] \cap K \cap M]^2$$
$$\times [\mathbf{Z}[x_0] \cap K : \mathbf{Z}[x_0] \cap K \cap M]^{-2} \min(M).$$

Moreover the index $[\mathbf{Z}[x_0] \cap K : \mathbf{Z}[x_0] \cap K \cap M]$ divides $[M_0 \cap (\sum_{i=1}^{r} M_i) : M]$.

Proof. It is easy to see

$$\prod_{i=1}^{r} Q(x_i) \geq \det(B(x_i, x_j))_{i,j \geq 1} = dK$$
$$= d(K + \mathbf{Z}[x_0])[K + \mathbf{Z}[x_0] : K]^2.$$

Moreover the index $[\mathbf{Z}[x_0] : \mathbf{Z}[x_0] \cap M]x_0 \in M$ implies $[\mathbf{Z}[x_0] : \mathbf{Z}[x_0] \cap M]^2 Q(x_0) \geq \min(M)$. Hence we have

$$\prod_{i=0}^{r} Q(x_i) \geq d(K + \mathbf{Z}[x_0])\,[K + \mathbf{Z}[x_0] : K]^2 [\mathbf{Z}[x_0] : \mathbf{Z}[x_0] \cap M]^{-2} \min(M).$$

Here we have

$$\begin{aligned} &[K + \mathbf{Z}[x_0] : K]\,[\mathbf{Z}[x_0] : \mathbf{Z}[x_0] \cap M]^{-1} \\ &= [\mathbf{Z}[x_0] : \mathbf{Z}[x_0] \cap K]\,[\mathbf{Z}[x_0] : \mathbf{Z}[x_0] \cap M]^{-1} \\ &= [\mathbf{Z}[x_0] \cap M : \mathbf{Z}[x_0] \cap K \cap M]\,[\mathbf{Z}[x_0] \cap K : \mathbf{Z}[x_0] \cap K \cap M]^{-1}, \end{aligned}$$

which implies the required inequality. Since the canonical mapping

$$(\mathbf{Z}[x_0] \cap K)/(\mathbf{Z}[x_0] \cap K \cap M) \rightarrow \Big(M_0 \cap (\sum_{i=1}^{r} M_i)\Big)/M$$

is injective, it completes the proof. □

COROLLARY. *Let M be a lattice on a positive definite quadratic space V over $\mathbf{Q}$ of $\dim V = m$. Let M_i $(i = 0, \ldots, m)$ be a lattice containing M on V such that $s(M_i) \subset \mathbf{Z}$ for $i = 0, \ldots, m$ and $[M_i : M]$ and $[M_j : M]$ are relatively prime if $i \neq j$. Then we have*

$$\min(M) \leq \prod_{i=0}^{m} \min(M_i).$$

In particular, $\min(M_i) \geq (\min(M))^{1/(m+1)}$ for some i.

Proof. Let $x_i \in M_i$ give the minimum and may assume that $K := \mathbf{Z}[x_1, \ldots, x_r]$ is a module of rank r and $x_0 \in \mathbf{Q}K$ without loss of generality. Then Proposition yields

$$\begin{aligned} \prod_{i=0}^{r} \min(M_i) &\geq d(K + \mathbf{Z}[x_0])\,[\mathbf{Z}[x_0] \cap M : \mathbf{Z}[x_0] \cap K \cap M]^2 \\ &\quad \times [\mathbf{Z}[x_0] \cap K : \mathbf{Z}[x_0] \cap K \cap M]^{-2} \min(M) \\ &\geq d(K + \mathbf{Z}[x_0])\,[\mathbf{Z}[x_0] \cap K : \mathbf{Z}[x_0] \cap K \cap M]^{-2} \min(M). \end{aligned}$$

On the other hand, the assumption implies $s(K + \mathbf{Z}[x_0]) \subset s(\sum_{i=0}^{m} M_i) \subset \mathbf{Z}$ and hence $d(K + \mathbf{Z}[x_0]) \geq 1$. Moreover $M_0 \cap (\sum_{i=1}^{m} M_i) = M$ implies $[\mathbf{Z}[x_0] \cap K : \mathbf{Z}[x_0] \cap K \cap M] = 1$, which completes the proof. □

Remark. *In the inequality, we need $m + 1$ lattices in general. For example, let $p_1 < \cdots < p_m$ be odd different primes, and $M = \mathbf{Z}[v_1, \ldots, v_m]$ with $(B(v_i, v_j)) = \mathrm{diag}(p_1^2, \ldots, p_m^2)$. We put*

https://doi.org/10.1017/S0027763000004773 Published online by Cambridge University Press

$$M_i = \mathbf{Z}[v_1, \ldots, v_{i-1}, p_i^{-1} v_i, v_{i+1}, \ldots, v_m].$$

Then $[M_i : M] = p_i$ *and* $\min(M_i) = 1$ *are clear and* $\min(M) \leq \Pi_{i=1}^m \min(M_i)$ *does not hold.*

REFERENCES

[1] J. S. Hsia, Y. Kitaoka and M. Kneser, Representations of positive definite quadratic forms, J. reine angew. Math., **301** (1978), 132–141.

[2] Y. Kitaoka, "Lectures on Siegel modular forms and representation by quadratic forms," Springer-Verlag, Heidelberg, 1986.

[3] ——, Local densities of quadratic forms, in "Investigations in Number theory (Advanced Studies in Pure Math.)," 1987 pp. 433–460.

[4] ——, Some remarks on representations of positive definite quadratic forms, Nagoya Math. J., **115** (1989), 23–41.

[5] ——, "Arithmetic of quadratic forms," Cambridge University Press, 1993.

[6] O. T. O'Meara, "Introduction to quadratic forms," Springer-Verlag, 1963.

Department of Mathematics
Nagoya University
Chikusa-ku Nagoya 464-01
Japan