Advanced Studies in Pure Mathematics 13, 1988
Investigations in Number Theory
pp. 433–460

Local Densities of Quadratic Forms

Yoshiyuki Kitaoka

Dedicated to Professor I. Satake on his 60th birthday

Introduction

Let $A^{(m)}$, $B^{(n)}$ be integral positive definite matrices. Our problem is to study when the quadratic equation $A[X]=B$ has an integral solution. We know already that $A[X]=B$ has an integral solution provided that $m\geqq 2n+3$, it has an integral solution over Z_p and $\min_{0\neq x\in Z^n} B[x]$ is sufficiently large. But we know nothing about this problem for $m\leqq 2n+2$ except in the case of $n=1$. To have a perspective, we know empirically that it is better to study the magnitude of the number $r(B, A)$ of integral solutions of $A[X]=B$. Siegel showed that the weighted average of $r(B, A_i)$ for $A_i \in \text{gen}\, A$ is an infinite product of the amount $\alpha_p(B, A)$ of local solutions, roughly speaking. Hence the local density $\alpha_p(B, A)$ may suggest something global. If, for example, the average is relatively large, that is, $\prod_p \alpha_p(B, A)>\kappa(>0)$, then we can expect $r(B, A')>0$ for every A' in $\text{gen}\, A$. If, to the contrary, the average is relatively small, then we may expect that it is almost equal to $r(B, A'')$ for some A'' in $\text{gen}\, A$, in other words, $r(B, A')/r(B, A'')$ may be sufficiently small for every A' in $\text{gen}\, A$ with $\text{cls}\, A'\neq \text{cls}\, A''$, and it leads us to the linear independence of theta series like in the case of $m=n+1$ (cf. the conjectures in [2, 3, 13]). Although there is a gap between the behaviour of the infinite product $\prod_p \alpha_p(B, A)$ and the one of each $\alpha_p(B, A)$, we want to give sufficient conditions in order that $\lim_i \alpha_p(B_i, A)=0$ or $\lim_i \inf \alpha_p(B_i, A)>0$ at the outset.

Theorem A. *Let M, $N=N_1\perp N_2$ be regular quadratc lattices over Z_p and let $\{M_i\}_{i=1}^s$ be representatives of submodules in M isometric to N_1 which are not transformed mutually by isometries of M. Then there are positive constants $c_i(N_1, M_i)$ such that*

$$\alpha_p(N, M)=\sum_i c_i(N_1, M_i)\alpha_p(N_2, M_i^{\perp}).$$

Hence the behaviour of $\alpha_p(N_1\perp N_2, M)$ with N_1 fixed is reduced to the one of $\alpha_p(N_2, M_i^{\perp})$.

Received October 7, 1986.

Theorem B. *Let M, N be regular quadratic lattices over $\boldsymbol{Z}_p$ with* $\mathrm{rk}\, N=n<\mathrm{rk}\, M=m$ *and* $N\subset M$.

a) *If there is a submodule N_0 of M such that $N_0\cong N$ and $[M\cap \boldsymbol{Q}_p N_0: N_0]<c_1$, then $\alpha_p(N, M)>c_2$ for a positive constant c_2 depending only on M, c_1.*

b) *If $m\geqq 2n+1$ and $\alpha_p(N, M)>c_1'$ (>0), then there is a submodule N' of M such that $N'\cong N$ and $[M\cap \boldsymbol{Q}_p N': N']<c_2'$ for some constant c_2' depending only on M, c_1'.*

If $m\geqq 2n+3$, then the assumption of a) holds and hence $\alpha_p(N, M)>c_1$ (>0) for $N\subset M$. This corresponds just to the global fact stated at the very beginning from the viewpoint of an analytic approach. For $m\geqq 2n+1$, the local density is away from zero if and only if an almost primitive representation of N by M exists. Does this suggest that the above global fact holds for primitive representations if $m\geqq 2n+1$? The spinor exceptions must be taken account of in the case of $m=3$, $n=1$.

Theorem C. *Let $M\supset N$ be regular quadratic lattices with* $\mathrm{rk}\, M=m$, $\mathrm{rk}\, N=n$, $\mathrm{ind}\, M=r$ *and suppose $n+1\leqq m\leqq 2n$. Then there is a positive constant $c(M, N)$ such that $\alpha_p(p^t N, M)>c(M, N)p^{t(n-r)(n+r+1-m)}$ for $t\geqq 0$.*

Unless $n=r+2$, $m=2n$, it is easy to see $(n-r)(n+r+1-m)\geqq 0$. If $n=r+2$ and $m=2n$, then $\alpha_p(p^t N, M)>c(M, N)p^{-2t}$ holds. The almost converse inequality $\alpha_p(p^t N, M)<cp^{(\varepsilon-2)t}$ holds for any $\varepsilon>0$ if the following holds:

Put

$$\begin{bmatrix} k \\ g \end{bmatrix} = \frac{\prod_{1\leqq i\leqq k}(1-q^i)}{\prod_{1\leqq i\leqq g}(1-q^i)\cdot \prod_{1\leqq i\leqq k-g}(1-q^i)} \quad \text{(Gaussian polynomial)},$$

$$H_n(x)=\sum_{r=0}^{n}\begin{bmatrix} n \\ r \end{bmatrix} x^r,$$

and define $F(a, k, z)$ inductively:

$$F(0, k, z)=\sum_{0\leqq g\leqq k}(-1)^{k-g}H_{k-g}(-q)\begin{bmatrix} k \\ g \end{bmatrix} q^{g(g+3)/2-k}z^g-1,$$

$$F(a+1, k, z)=\sum_{a+1\leqq g\leqq k}F(a, g, z)(-1)^{k-g}H_{k-g}(-q)\begin{bmatrix} k \\ g \end{bmatrix} q^{g(g+3)/2-k}z^g$$
$$-F(a, k, z)q^{(a+1)(a+2)/2}z^{a+1}.$$

If, then $F(n-2, n-1, q^{-n})=F(n-2, n, q^{-n})=0$ $(n=\mathrm{rk}\, N)$ holds, then the above almost converse inequality holds, and it is the case if $n\leqq 9$.

It may be interesting to study the case when $\alpha_q(N_i, M)\to 0$ (or $\to\infty$) and $\alpha_p(N_i, M)<c_p$ (or $>c_p$) for some constant c_p for every prime $p\neq q$.

It might be a next problem to give a sufficient and/or necessary condition to $\lim \alpha_p(K, M)=0$, $\underline{\lim}\, \alpha_p(K, M)>0$ where K runs over submodules in a fixed lattice.

We denote by $\boldsymbol{Z}_p$, $\boldsymbol{Q}_p$ the ring of p-adic integers, the field of p-adic numbers respectively. For a quadratic lattice M over $\boldsymbol{Z}_p$, $Q(x)$, $B(x, y)$ are the quadratic form and the bilinear form on it with $Q(x+y)-Q(x)-Q(y)=2B(x, y)$. $M^\#$ is, by definition, $\{x\in \boldsymbol{Q}_pM \mid B(x, M)\subset \boldsymbol{Z}_p\}$. $\mathfrak{n}(M)$, $\mathfrak{s}(M)$ denote $\boldsymbol{Z}_p\{Q(x)\mid x\in M\}$, $\{B(x, y)\mid x, y\in M\}$ respectively and then $2\mathfrak{s}(M)\subset\mathfrak{n}(M)\subset\mathfrak{s}(M)$ is obvious.

§1.

In this section we define the local density for the sake of completeness, and give a reduction formula.

Let $M=\boldsymbol{Z}_p[u_1, \cdots, u_m]$, $N=\boldsymbol{Z}_p[v_1, \cdots, v_n]$ be regular quadratic lattices over $\boldsymbol{Z}_p$ with rank $M=m\geqq$ rank $N=n$, and suppose that there is a submodule $K=\boldsymbol{Z}_p[w_1, \cdots, w_n]$ of M which is isometric to N. These are fixed through this section.

We put

$$A_{p^t}(N, M)=\left\{\sigma: N\longrightarrow M/p^tM^\# \;\middle|\; \begin{array}{l}\sigma \text{ is a linear mapping with } Q(\sigma x)\\ \equiv Q(x) \bmod 2p^t\boldsymbol{Z}_p \text{ for } x\in N\end{array}\right\},$$

$$B_{p^t}(N, M)=\left\{\sigma: N\longrightarrow M/p^tM \;\middle|\; \begin{array}{l}\sigma \text{ is a linear mapping with } Q(\sigma x)\\ \equiv Q(x) \bmod 2p^t\boldsymbol{Z}_p \text{ for } x\in N\end{array}\right\},$$

$$C_{p^t}(N, M)=\left\{\sigma: N\longrightarrow M/p^tM \;\middle|\; \begin{array}{l}\sigma \text{ is a linear mapping with } B(\sigma x, \sigma y)\\ \equiv B(x, y) \bmod p^t\boldsymbol{Z}_p \text{ for } x, y\in N\end{array}\right\},$$

$$D_{p^t}(N, M)=\left\{\sigma\in A_{p^t}(N, M) \;\middle|\; \begin{array}{l}\sigma \text{ induces an injective mapping}\\ \text{from } N/pN \text{ to } M/pM\end{array}\right\},$$

$$E_{p^t}(N, M)=\left\{\sigma\in B_{p^t}(N, M) \;\middle|\; \begin{array}{l}\sigma \text{ induces an injective mapping}\\ \text{from } N/pN \text{ to } M/pM\end{array}\right\},$$

$$F_{p^t}(N, M; K)=\left\{\sigma\in C_{p^t}(N, M) \;\middle|\; \begin{array}{l}\text{There is an isometry } \eta \text{ of } M \text{ such}\\ \text{that } \eta(K)=\boldsymbol{Z}_p[\sigma(v_1), \cdots, \sigma(v_n)]\end{array}\right\}.$$

Proposition 1. *Let h_N, h_M be integers such that $p^{h_N}\mathfrak{n}(N^\#)\subset 2\boldsymbol{Z}_p$, $p^{h_M}\mathfrak{n}(M^\#)\subset 2\boldsymbol{Z}_p$ respectively. Then the following assertions hold where $\mathfrak{n}(M)\subset 2\boldsymbol{Z}_p$ is supposed in* (ii)$\sim$(v).

(i) *For $t\geqq h_M$, $A_{p^t}(N, M)$ is well-defined.*

(ii) *$B_{p^t}(N, M)$ is well-defined for $t\geqq 0$ and $(p^t)^{n(n+1)/2-mn}\,\sharp B_{p^t}(N, M)$ is constant for $t\geqq h_N+1$, and $\sharp B_{p^t}(N, M)=[M^\#: M]^n\,\sharp A_{p^t}(N, M)$ if $t\geqq h_M$.*

(iii) *$C_{p^t}(N, M)$ is well-defined for $t \geqq 0$ and $(p^t)^{n(n+1)/2-mn} \# C_{p^t}(N, M)$ is constant if either $t \geqq h_N+1$ for $p \neq 2$,* or *$t \geqq h_N+2$ for $p=2$, and $\# C_{p^t}(N, M)=2^{n\delta_{2,p}} \# B_{p^t}(N, M)$ for $t \geqq 0$ if $p \neq 2$ and for $t \geqq h_N+2$ if $p=2$.*

(iv) *For $t \geqq h_M+1$, we have $\# E_{p^t}(N, M)=[M^\#: M]^n \# D_{p^t}(N, M)$, and $(p^t)^{n(n+1)/2-mn} \# D_{p^t}(N, M)$ is constant for $t \geqq h_M+1$.*

(v) *There is a constant a such that for $t \geqq a$, $F_{p^t}(N, M; K)$ is well-defined and $(p^t)^{n(n+1)/2-mn} \# F_{p^t}(N, M; K)$ is constant.*

Proof. Suppose $t \geqq h_M$; then we have $\mathfrak{s}(M^\#) \subset \frac{1}{2}\mathfrak{n}(M^\#) \subset p^{-t} Z_p$ and hence $B(M^\#, p^t M^\#) \subset Z_p$. Thus we have $p^t M^\# \subset (M^\#)^\# = M$. Moreover for $x \in M, y \in M^\#$ we have $Q(x+p^t y)=Q(x)+2p^t B(x, y)+p^{2t}Q(y) \equiv Q(x) \bmod 2p^t Z_p$. Thus $A_{p^t}(N, M)$ is well-defined. Suppose $\mathfrak{n}(M) \subset 2Z_p$. If $t \geqq h_M$, then $p^t M \subset p^t M^\# \subset M$ implies $\# B_{p^t}(N, M)=[p^t M^\#: p^t M]^n \# A_{p^t}(N, M)=[M^\#: M]^n \# A_{p^t}(N, M)$. Put $S=(B(u_i, u_j))$, $T=(B(v_i, v_j))$; then$\#$ $B_{p^t}(N, M)$ is the cardinality of the set $r(T, S; p^t)$ of $X \in M_{m,n}(Z_p/p^t Z_p)$ which satisfies that $S[X][x] \equiv T[x] \bmod 2p^t Z_p$ for every $x \in Z_p^n$. We claim that $p^{nm} \# r(T, S; p^t)=\sum_i \# r(T_i, S; p^{t+1})$ where $\{T_i\}$ runs over symmetric matrices such that $T_i[x] \equiv T[x] \bmod 2p^t Z_p$ for every $x \in Z_p^n$ and $x \rightarrow T_i[x] \bmod 2p^{t+1} Z_p$ gives a distinct mapping if $i \neq j$. This is clear, considering the mapping $X \rightarrow X$ from $\coprod_i r(T_i, S; p^{t+1})$ onto $r(T, S; p^t)$. By Corollary 1 on p. 180 in [6], there is $G_i \in GL_n(Z_p)$ such that $T_i=T[G_i]$ if $t \geqq h_N+1$, and then $\# r(T_i, S; p^{t+1})=\# r(T, S; p^{t+1})$. Since the cardinality of $\{T_i\}$ is $p^{n(n+1)/2}$, we have, for $t \geqq h_N+1$,

$$\# B_{p^t}(N, M)=p^{-nm+n(n+1)/2} \# B_{p^{t+1}}(N, M).$$

This completes the proof of (ii). Since $B_{p^t}(N, M)=C_{p^t}(N, M)$ for $p \neq 2$, we may suppose $p=2$ to prove the assertion (iii). By $r'(T, S; 2^{t+1})$ we denote the set $\{X \in M_{m,n}(Z_2/2^{t+1}Z_2) \mid S[X] \equiv T \bmod 2^{t+1} Z_2\}$. Let $\{T'_i\}$ be the set of $T'_i={}^t T'_i \in M_n(Z_2/2^{t+1}Z_2)$ which are distinct if $i \neq j$ and satisfies $T'_i[x] \equiv T[x] \bmod 2^{t+1} Z_2$ for every $x \in Z_2^n$. Considering the mapping $X \rightarrow X$ from $\coprod_i r'(T_i, S; 2^{t+1}) \rightarrow r(T, S; 2^t)$, we have

$$\sum_i \# r'(T_i, S; 2^{t+1})=2^{mn} \# r(T, S; 2^t),$$

and as above for $t \geqq h_N+1$ $\# r'(T_i, S; 2^{t+1})=\# r'(T, S; 2^{t+1})$ implies $2^{n(n-1)/2} \# r'(T, S; 2^{t+1})=2^{mn} \# r(T, S; 2^t)$. Thus we have, for $t \geqq h_N+1$,

$$\begin{aligned}\# C_{2^{t+1}}(N, M)&=\# r'(T, S; 2^{t+1})=2^{mn-n(n-1)/2} \# r(T, S; 2^t)\\ &=2^n \# r(T, S; 2^{t+1}).\end{aligned}$$

This completes the proof of the assertion (iii). The first assertion of (iv) is proved similarly to (ii). The second assertion follows from (14.2) and

(14.3) in [9], applying it to $N\to E$, $Q_pM\to H$, $G\to M^{\#}$, $u\in D_{p^t}(N, M)$. Lastly we show (v). Let $\sigma\in C_{p^t}(N, M)$ and y_i, $z_i\in M$ satisfy $y_i\equiv z_i\equiv \sigma(v_i) \bmod p^tM$. Since $B(y_i, y_j)\equiv B(v_i, v_j) \bmod p^t$, by virtue of Corollary 4 on p. 184 and its proof in [6], there is an isometry α of M such that $\alpha(Z_p[y_1, \cdots, y_n])=Z_p[z_1, \cdots, z_n]$. Thus $F_{p^t}(N, M; K)$ is well-defined for a sufficiently large t. Put $S=(B(u_i, u_j))$, $T=(B(v_i, v_j))$ and for $\sigma\in F_{p^t}(N, M; K)$ we take any element $y_i\in M$ such that $y_i\equiv\sigma(v_i) \bmod p^tM$, and define $Y\in M_{m,n}(Z_p)$ by $(y_1, \cdots, y_n)=(u_1, \cdots, u_m)Y$. Then for an isometry η in the definition of $F_{p^t}(N, M; K)$ $(\eta(w_1), \cdots, \eta(w_n))=(y_1, \cdots, y_n)G$ for some G in $GL_n(Z_p)$. Defining $A\in GL_m(Z_p)$, $Z\in M_{m,n}(Z_p)$ by $(\eta(u_1), \cdots, \eta(u_m))=(u_1, \cdots, u_m)A$, $(w_1, \cdots, w_n)=(u_1, \cdots, u_m)Z$, we have $(u_1, \cdots, u_m)AZ=(\eta(u_1), \cdots, \eta(u_m))Z=(\eta(w_1), \cdots, \eta(w_n))=(y_1, \cdots, y_n)G=(u_1, \cdots, u_m)YG$ and thus $AZ=YG$. It is easy to see that the mapping $\sigma\to Y$ is a bijection from $F_{p^t}(N, M; K)$ to $r(N, M; K; p^t)=\left\{Y\in M_{m,n}(Z_p) \bmod p^t \,\middle|\, \begin{matrix} S[Y]\equiv T \bmod p^t,\ YG=AZ \text{ for some } G \text{ in} \\ GL_n(Z_p) \text{ and } A\in GL_m(Z_p) \text{ with } S[A]=S \end{matrix}\right\}$. Since the second condition $YG=AZ$ holds also for every $Y'\equiv Y \bmod p^t$ for a sufficiently large t as noted above in terms of lattices, the assertion (v) is proved similarly to (ii).

We define the local densities by

$$\begin{aligned}\alpha_p(N, M)&=2^{n\delta_{2,p}-\delta_{m,n}}[M^{\#}: M]^n \lim_{t\to\infty} (p^t)^{n(n+1)/2-mn} \# A_{p^t}(N, M)\\ &=2^{n\delta_{2,p}-\delta_{m,n}} \lim_{t\to\infty} (p^t)^{n(n+1)/2-mn} \# B_{p^t}(N, M) \qquad \text{if } \mathfrak{n}(M)\subset 2Z_p\\ &=2^{-\delta_{m,n}} \lim_{t\to\infty} (p^t)^{n(n+1)/2-mn} \# C_{p^t}(N, M) \qquad \text{if } \mathfrak{n}(M)\subset 2Z_p,\end{aligned}$$

and in the case of $\mathfrak{n}(M)\subset 2Z_p$,

$$\begin{aligned}d_p(N, M)&=2^{-\delta_{m,n}} \lim_{t\to\infty} (p^t)^{n(n+1)/2-mn} \# E_{p^t}(N, M)\\ &=2^{-\delta_{m,n}}[M^{\#}: M]^n \lim_{t\to\infty} (p^t)^{n(n+1)/2-mn} \# D_{p^t}(N, M),\\ \alpha_p(N, M; K)&=\lim_{t\to\infty} (p^t)^{n(n+1)/2-mn} \# F_{p^t}(N, M; K).\end{aligned}$$

The following is due to Siegel.

Proposition 2. $\alpha_p(N, M)=2^{n\delta_{2,p}} \sum_{Q_pN\supset N_0\supset N} [N_0: N]^{n-m+1} d_p(N_0, M)$ *if* $\mathfrak{n}(M)\subset 2Z_p$.

Proof. Put $S=(B(u_i, u_j))$, $T=(B(v_i, v_j))$ and $\tilde{C}_{p^t}(T, S)=\{X\in M_{m,n}(Z_p) \bmod p^t \mid S[X]\equiv T \bmod p^t\}$. $\# \tilde{C}_{p^t}(T, S)=\# C_{p^t}(N, M)$ is clear. For $G\in GL_n(Q_p)\cap M_n(Z_p)$ we put $\tilde{C}_{p^t}(T, S; G)=\{X\in M_{m,n}(Z_p) \bmod p^t \mid S[X]\equiv T \bmod p^t, XG^{-1} \text{ is primitive}\}$ and then $\# \tilde{C}_{p^t}(T, S)=\sum_G \# \tilde{C}_{p^t}(T, S; G)$

where G runs over $GL_n(Z_p)\backslash GL_n(Q_p)\cap M_n(Z_p)$, noting that if $XG_i^{-1}(i=1,2)$ is primitive, then $G_1G_2^{-1}\in GL_n(Z_p)$ holds. Suppose $S[X]\equiv T \bmod p^t$ and XG^{-1} is primitive for $G\in GL_n(Q_p)\cap M_n(Z_p)$. Put $S[X]=T+p^tR$; then $R={}^tR\in M_n(Z_p)$ and $S[XG^{-1}]=T[G^{-1}]+p^tR[G^{-1}]$. Denote by $\{R_1,\cdots,R_a\}$ the representatives of the set $\{p^tR[G^{-1}]\,|\,R={}^tR\in M_n(Z_p)\}\bmod\{p^tR\,|\,R={}^tR\in M_n(Z_p)\}$. Then we have $S[XG^{-1}]\equiv T[G^{-1}]+R_i \bmod p^t$ for some i. Since $|T|\equiv|S[XG^{-1}]|\,|G|^2 \bmod p^t$, we have $2\,\mathrm{ord}\,|G|\leqq \mathrm{ord}\,|T|$ if $t>\mathrm{ord}\,|T|$, and then R_i and hence $T[G^{-1}]$ are integral for a sufficiently large t. The mapping $X\mapsto XG^{-1}$ is a bijection from

$$\tilde{C}'_{p^t}(T,S;G)=\left\{X\in M_{m,n}(Z_p) \bmod p^tM_{m,n}(Z_p)G \,\middle|\, \begin{matrix} S[X]\equiv T \bmod p^t \\ XG^{-1} \text{ is primitive}\end{matrix}\right\}$$
$$\longrightarrow \coprod_i \tilde{C}_{p^t}(T[G^{-1}]+R_i,S;1_n).$$

For a sufficiently large t, $R_i\equiv 0 \bmod p^{[t/2]}$ holds and then $T[G^{-1}]+R_i=T[G^{-1}][G']$ for some $G'\in GL_n(Z_p)$. Thus we have

$$\begin{aligned}\#\tilde{C}'_{p^t}(T,S;G)&=\sum_i \#\tilde{C}_{p^t}(T[G^{-1}],S;1_n)\\ &=(p^{\mathrm{ord}|G|})^{n+1}\#\tilde{C}_{p^t}(T[G^{-1}],S;1_n)\\ &=(p^{\mathrm{ord}|G|})^{n+1}2^{n\delta_{2,p}}\\ &\quad\times\#\left\{X \bmod p^t \,\middle|\, \begin{matrix} S[X][x]\equiv T[G^{-1}x] \bmod 2p^tZ_p \text{ for} \\ \text{every } x\in Z_p^n \text{ and } X \text{ is primitive}\end{matrix}\right\}\end{aligned}$$

as in the proof of (iii) in Proposition 1,

$$=(p^{\mathrm{ord}|G|})^{n+1}2^{n\delta_{2,p}}\#E_{p^t}(T[G^{-1}],M),$$

identifying $T[G^{-1}]$ with the quadratic lattice corresponding to it. Since $\#\tilde{C}'_{p^t}(T,S;G)=(p^{\mathrm{ord}|G|})^m\#\tilde{C}_{p^t}(T,S;G)$, we have $\#C_{p^t}(N,M)=\#\tilde{C}_{p^t}(T,S)=\sum_G\#\tilde{C}_{p^t}(T,S;G)=\sum_G(p^{\mathrm{ord}|G|})^{n+1-m}2^{n\delta_{2,p}}\#E_{p^t}(T[G^{-1}],M)$. Using terms of lattices, we complete the proof.

Remark. By (iv) of the previous proposition, there exist constants c_1, c_2 dependent only on M such that $c_1<d_p(N,M)<c_2$ if $d_p(N,M)\neq 0$. Hence we have

$$\begin{aligned}\alpha_p(N,M)\underset{\cap}{\overset{\cup}{\sim}}&\sum_{\substack{Q_pN\supset N_0\supset N\\ d_p(N_0,M)\neq 0}}[N_0:N]^{n-m+1}\\ &=\sum_H p^{(n-m+1)/2\cdot\mathrm{ord}(dN/dH)}\#\{L\,|\,Q_pN\supset L\supset N,\ L\cong H\},\end{aligned}$$

where H runs over representatives of isometry classes of primitive submodules of rank$=n$ of M. On the other hand, the proposition implies directly $\alpha_p(N, M)=2^{n\delta_{2,p}}d_p(M, M)p^{\mathrm{ord}(dN/dM)/2}\#\{N_0 \mid \boldsymbol{Q}_pN\supset N_0\supset N, N_0\cong M\}$ if $n=m$.

If $n=m=2$, then the following is easily shown by checking the reduction formula in [5].

Suppose $p\neq 2$ and $N=\langle\varepsilon_1p^{A_1}\rangle\perp\langle\varepsilon_2p^{A_2}\rangle$, $M=\langle\delta_1p^{B_1}\rangle\perp\langle\delta_2p^{B_2}\rangle$, where ε_1, ε_2, δ_1, δ_2 are p-adic units in $\boldsymbol{Z}_p$ with $\varepsilon_1\varepsilon_2=\delta_1\delta_2$ and $0\leqq A_1\leqq A_2$, $0\leqq B_1\leqq B_2$, $A_1+A_2\equiv B_1+B_2 \bmod 2$, $A_1\geqq B_1$, $A_2\geqq B_2$. (These conditions are necessary to $\alpha_p(N, M)\neq 0$.) Then we have

$$\alpha_p(N, M)/\alpha_p(M, M)$$

$$=\begin{cases}\frac{1}{2}(1+\chi(\varepsilon_1\delta_1))p^{A_1-B_1+(A_2-B_2)/2} & \text{if } A_1<B_2,\\ & \quad A_i\equiv B_i \bmod 2\ (i=1, 2).\\ 0 & \text{if } A_1<B_2, \text{ and either}\\ & \quad A_1\not\equiv B_1 \bmod 2 \text{ or}\\ & \quad A_2\not\equiv B_2 \bmod 2,\\ \frac{1}{2}(1+\chi(\varepsilon_1\delta_1))p^{(A_1+A_2-1)/2-B_1} & \text{if } B_1\not\equiv B_2 \bmod 2,\ B_2\leqq A_1 \text{ and}\\ & \quad A_1\equiv B_1 \bmod 2,\\ \frac{1}{2}(1+\chi(\varepsilon_2\delta_1))p^{(A_1+A_2-1)/2-B_1} & \text{if } B_1\not\equiv B_2 \bmod 2,\ B_2\leqq A_1 \text{ and}\\ & \quad A_1\not\equiv B_1 \bmod 2,\\ p^{(A_1+A_2)/2-B_2}\left(\sum_{r=0}^{A_1-B_2}\chi(-\varepsilon_1\varepsilon_2)^r\right) & \\ \quad\times\begin{cases}\frac{1}{2}p^{B_2-B_1-1}(p-\chi(-\varepsilon_1\varepsilon_2)) & \text{if } B_1\equiv B_2 \bmod 2,\ B_2\leqq A_1 \text{ and}\\ & \quad B_1<B_2,\\ 1 & \text{if } B_1\equiv B_2 \bmod 2,\ B_2\leqq A_1 \text{ and}\\ & \quad B_1=B_2,\end{cases} & \end{cases}$$

where $\chi(\varepsilon)=\left(\frac{\varepsilon}{p}\right)$ (Legendre symbol).

We give another reduction formula.

Proposition 3. *Suppose* $\mathfrak{n}(M)\subset 2\boldsymbol{Z}_p$ *and* $N=N_1\perp N_2$ *with* $\mathrm{rk}\, N_i=n_i>0$ $(i=1, 2)$ *and let* $\{M_i\}_{i=1}^{s}$ *be representatives of submodules of* M *isometric to* N_1 *which are not transformed mutually by isometries of* M. *Then we have*

$$\alpha_p(N, M)=\sum_{i=1}^{s}([M_i^\sharp: M_i]/[M: M_i\perp M_i^\perp])^{n_2}\alpha_p(N_1, M; M_i)\alpha_p(N_2, M_i^\perp).$$

Lemma 1. *We have, for a sufficiently large* t

$$\# C_{p^t}(N, M)=\sum_{i=1}^{s} \# F_{p^t}(N_1, M; M_i)\cdot \#\{\sigma_2 \in C_{p^t}(N_2, M) \mid B(M_i, \sigma_2 N_2)\equiv 0(p^t)\}.$$

Proof. For σ_1 in $C_{p^t}(N_1, M)$ we take and fix $\sigma_1(x_i)$ as an element of M where $\{x_i\}$ is a basis of N_1, and fix an isometry α of M such that $\alpha \boldsymbol{Z}_p[\sigma_1(x_1), \cdots, \sigma_1(x_{n_1})]=M_i$ for some i. Suppose that $\sigma \in C_{p^t}(N, M)$ is given, and put $\sigma_1=\sigma|_{N_1}$ which is in $F_{p^t}(N_1, M; M_i)$ for some i. For α, M_i corresponding to σ_1 as above, we put $\sigma_2=\alpha\sigma|_{N_2}$. Then $B(N_1, N_2)=0$ implies $B(M_i, \sigma_2(N_2))\equiv 0 \bmod p^t$, and the correspondence $\sigma \to (\sigma_1, \sigma_2)$ is injective from $C_{p^t}(N, M)$ to

$$\coprod_i F_{p^t}(N_1, M; M_i)\times\{\sigma_2 \in C_{p^t}(N_2, M) \mid B(M_i, \sigma_2(N_2))\equiv 0 \bmod p^t\}.$$

Conversely for $\sigma_1 \in F_{p^t}(N_1, M; M_i)$, $\sigma_2 \in C_{p^t}(N_2, M)$ with $B(M_i, \sigma_2(N_2)) \equiv 0 \bmod p^t$ we get $\sigma=\sigma_1 \perp \alpha^{-1}\sigma_2 \in C_{p^t}(N, M)$. Thus the mapping is surjective.

Lemma 2. $\#\{\sigma_2 \in C_{p^t}(N_2, M) \mid B(M_i, \sigma_2 N_2)\equiv 0 \bmod p^t\}$
$=([M_i^\#: M_i]/[M: M_i \perp M_i^\perp])^{n_2} \# C_{p^t}(N_2, M_i^\perp)$.

Proof. We claim $\{x \in M \mid B(M_i, x)\equiv 0 \bmod p^t\}=p^t M_i^\# \perp M_i^\perp$. The left contains clearly the right, noting that $p^t M_i^\# \subset M$ for a sufficiently large t. Conversely suppose that $x \in M$ satisfy $B(M_i, x)\equiv 0 \bmod p^t$, and decompose $x=x_1+x_2$, $x_1 \in \boldsymbol{Q}_p M_i$, $x_2 \in \boldsymbol{Q}_p M_i^\perp$. Then $B(M_i, x)=B(M_i, x_1) \equiv 0 \bmod p^t$ follows and hence we have $x_1 \in p^t M_i^\# \subset M$. Thus $x_2=x-x_1 \in M \cap \boldsymbol{Q}_p M_i^\perp=M_i^\perp$ holds. Taking an integer a such that $p^a M_i^\# \subset M_i \subset M$, we have

$$\begin{aligned}
&\#\{\sigma_2 \in C_{p^t}(N_2, M) \mid B(M_i, \sigma_2 N_2)\equiv 0(p^t)\}\\
&=\#\{\sigma_2 \in C_{p^t}(N_2, M) \mid \sigma_2(N_2)\subset p^t M_i^\# \perp M_i^\perp\}\\
&=[M: p^a M_i^\# \perp M_i^\perp]^{-n_2}\\
&\quad\times \#\left\{\sigma_2: N_2 \longrightarrow p^t M_i^\# \perp M_i^\perp / p^t(p^a M_i^\# \perp M_i^\perp) \;\middle|\; \begin{array}{l}\sigma_2 \text{ is linear and}\\ B(\sigma_2 x, \sigma_2 y)\equiv\\ B(x, y) \bmod p^t\\ \text{for any } x, y \in N_2.\end{array}\right\}.
\end{aligned}$$

Write $\sigma_2(x)=\gamma_1(x)+\gamma_2(x)$ with $\gamma_1(x) \in p^t M_i^\# / p^{t+a} M_i^\#$, $\gamma_2(x) \in M_i^\perp / p^t M_i^\perp$; then we have $B(\gamma_1(x), \gamma_1(y))\equiv 0 \bmod p^{2t}\mathfrak{s}(M_i^\#)$ and $p^{2t}\mathfrak{s}(M_i^\#)=p^{2(t-a)}\mathfrak{s}(p^a M_i^\#) \subset p^{2(t-a)}\mathfrak{s}(M_i)\subset p^{t+(t-2a)}\boldsymbol{Z}_p \subset p^t \boldsymbol{Z}_p$ for $t \geqq 2a$. Thus we have

$$\begin{aligned}
&\#\{\sigma_2 \in C_{p^t}(N_2, M) \mid B(M_i, \sigma_2 N_2)\equiv 0 \bmod p^t\}\\
&=[M: p^a M_i^\# \perp M_i^\perp]^{-n_2} p^{a n_1 n_2} \# C_{p^t}(N_2, M_i^\perp).
\end{aligned}$$

$$p^{an_1}/[M: p^a M_i^\# \perp M_i^\perp] = p^{an_1}/[M: M_i \perp M_i^\perp][M_i \perp M_i^\perp : p^a M_i^\# \perp M_i^\perp]$$
$$= [M_i^\#: M_i]/[M: M_i \perp M_i^\perp]$$

completes the proof of the lemma and then the proposition, combining with the previous lemma.

Remark. In the proposition, $[M_i^\#: M_i]/[M: M_i \perp M_i^\perp]$ is integral, and it is not hard to see that

$$\alpha_p(N, M; K)$$
$$= [M \cap \mathbf{Q}_p K: K]^{n+1-m} \# (O(K)/O(K) \cap O(M \cap \mathbf{Q}_p K))$$
$$\times \lim_{t\to\infty} (p^t)^{n(n+1)/2-mn} \# \left\{ \sigma: M \cap \mathbf{Q}_p K \longrightarrow M/p^t M \;\middle|\; \begin{array}{l} \sigma \text{ is linear and } B(\sigma x, \sigma y) \\ \equiv B(x, y) \bmod p^t \mathbf{Z}_p \text{ for} \\ x, y \in M \cap \mathbf{Q}_p K, \\ \text{and there is } \eta \in O(M) \\ \text{such that } \eta\sigma K = K, \\ \eta\sigma(M \cap \mathbf{Q}_p K) = M \cap \mathbf{Q}_p K \end{array} \right\}$$

where $O(*)$ means the group of isometries of $*$.

§ 2.

Proposition 4. *Let M, M', N and N' be regular quadratic lattices over $\mathbf{Z}_p$ with* $\operatorname{rk} M = \operatorname{rk} M' = m$, $\operatorname{rk} N = \operatorname{rk} N' = n$. *Then we have*

a) $\alpha_p(p^r N, p^r M) = p^{rn(n+1)} \alpha_p(N, M)$,

b) *if* $M \subset M'$, *then* $\alpha_p(N, M) \leqq [M': M]^n \alpha(N, M')$,

c) *if* $M \subset M'$ *and* $p^r M' \subset M$,

then $\alpha_p(N, M') \leqq p^{-rn(n+1)} [M: p^r M']^n \cdot \alpha_p(p^r N, M)$,

d) *if* $N \subset N'$, *then* $\alpha_p(N', M) \leqq [N': N]^{m-n-1} \alpha_p(N, M)$,

e) *if* $M' \subset M$ *and for every isometry* σ *from* N *to* M, $\sigma(N)$ *is contuined in* M', *then* $\alpha_p(N, M) = [M: M']^{-n} \alpha_p(N, M')$.

Proof. For the assertion a) we may suppose $r \geqq 0$. For a sufficiently large t, we have

$$\alpha_p(p^r N, p^r M)$$
$$= 2^{n\delta_{2,p} - \delta_{m,n}} [(p^r M)^\#: p^r M]^n (p^t)^{n(n+1)/2-mn} \# A_{p^t}(p^r N, p^r M)$$
$$= 2^{n\delta_{2,p} - \delta_{m,n}} p^{2rmn} [M^\#: M]^n (p^t)^{n(n+1)/2-mn} \# A_{p^{t-2r}}(N, M)$$
$$= 2^{n\delta_{2,p} - \delta_{m,n}} [M^\#: M]^n (p^{t-2r})^{n(n+1)/2-mn} \# A_{p^{t-2r}}(N, M) p^{rn(n+1)}$$
$$= p^{rn(n+1)} \alpha_p(N, M).$$

By virtue of a) we may assume $\mathfrak{n}(M)$, $\mathfrak{n}(M') \subset 2\mathbf{Z}_p$ for the assertions b) ~

e). Using the canonical mapping i: $M/p^tM \to M'/p^tM'$, we define the mapping $\varphi \to i \circ \varphi$ from $C_{p^t}(N, M)$ to $C_{p^t}(N, M')$. Since $\#\{\varphi: N \to M/p^tM \mid \varphi$ is linear and $i \circ \varphi = 0\} = [M': M]^n$, we have $\# C_{p^t}(N, M) = \sum_{i\circ\varphi} \#\{\varphi' \in C_{p^t}(N, M) \mid i \circ \varphi' = i \circ \varphi\} \leqq [M': M]^n \# C_{p^t}(N, M')$ and this completes the proof of b). For c) we have

$$\begin{aligned}\alpha_p(N, M') &= p^{-rn(n+1)}\alpha_p(p^rN, p^rM') && \text{by a)}\\ &\leqq p^{-rn(n+1)}[M: p^rM']^n\alpha_p(p^rN, M) && \text{by b).}\end{aligned}$$

For d), from Proposition 2 follows

$$\begin{aligned}\alpha_p(N, M) &= 2^{n\delta_{2,p}} \sum_{Q_pN \supset N_0 \supset N} [N_0: N]^{n-m+1} d_p(N_0, M)\\ &\geqq 2^{n\delta_{2,p}} \sum_{Q_pN' \supset N_0 \supset N'} [N_0: N']^{n-m+1} d_p(N_0, M)[N': N]^{n-m+1}\\ &= [N': N]^{n-m+1}\alpha_p(N', M).\end{aligned}$$

For e) we fix a natural number h such that $p^h\mathfrak{n}(N^\#) \subset 2\boldsymbol{Z}_p$. For an integer t greater than h and $\sigma \in B_{p^t}(N, M)$, there is an isometry σ' from N to M such that $\sigma'(N) = \sigma(N)$ by virtue of Corollary 1 on p. 180 in [6], considering σ as a homomorphism from N to M. Since $\sigma'(N) \subset M'$ follows from the assumption, we have $\sigma(N) \subset M'$. Thus we have

$$\begin{aligned}\# B_{p^t}(N, M) &= \#\{\sigma \in B_{p^t}(N, M) \mid \sigma(N) \subset M'\}\\ &= [M: M']^{-n} \# B_{p^t}(N, M'),\end{aligned}$$

and hence

$$\alpha_p(N, M) = [M: M']^{-n}\alpha_p(N, M').$$

Theorem 1. *Let N, M be regular quadratic lattices over $\boldsymbol{Z}_p$ with* $\operatorname{rk} N = n < \operatorname{rk} M = m$ *and $N \subset M$, and c a positive number.*

a) *If there is a submodule N_0 of M such that $N_0 \cong N$ and $[M \cap \boldsymbol{Q}_pN_0: N_0] < c$, then $\alpha_p(N, M) > c(M)c^{n+1-m}$ holds for positive constant $c(M)$ dependent only on M.*

b) *If $m \geqq 2n+1$ and $\alpha_p(N, M) > c$, then there is a submodule N' of M such that $N' \cong N$ and $[M \cap \boldsymbol{Q}_pN': N'] < c'(M)$ for some constant $c'(M)$ dependent only on M, c.*

Proof. Since

$$\begin{aligned}\alpha_p(N, M) &= \alpha_p(N_0, M)\\ &= 2^{n\delta_{2,p}} \sum_{Q_pN_0 \supset K \supset N_0} [K: N_0]^{n-m+1} d_p(K, M)\\ &\geqq 2^{n\delta_{2,p}}[M \cap \boldsymbol{Q}_pN_0: N_0]^{n-m+1} d_p(M \cap \boldsymbol{Q}_pN_0, M),\end{aligned}$$

we have only to define $c(M)$ by $\min_{\mathrm{rk}\,K=n, d_p(k,M)\neq 0} 2^{n\delta_{2,p}} d_p(K, M)$, noting that $d_p(K, M)$ can take only a finite number of values. To prove b), we put $r=\min_{\substack{Q_pN\supset N_0\supset N\\ d_p(N_0,M)\neq 0}} \mathrm{ord}\,[N_0\colon N]$ and suppose $m\geqq 2n+1$. Then

$$\begin{aligned}\alpha_p(N, M) &= 2^{n\delta_{2,p}} \sum_{Q_pN\supset N_0\supset N} [N_0\colon N]^{n-m+1} d_p(N_0, M)\\ &\leqq 2^{n\delta_{2,p}} \max_{Q_pN\supset N_0\supset N} d_p(N_0, M) \sum_{s\geqq r} p^{s(n-m+1)} A(n, s),\end{aligned}$$

where $A(n, s)$ is the number of lattices over Z_p which contains a given lattice with index p^s, and $A(n, s)\leqq(1-p^{-1})^{1-n}p^{(n-1)s}$ is easy,

$$\begin{aligned}&\leqq c_1(M) \sum_{s\geqq r} p^{s(2n-m)}\\ &\leqq c_2(M) p^{r(2n-m)}.\end{aligned}$$

Thus we have $c<\alpha_p(N, M)<c_2(M)p^{r(2n-m)}$ and hence

$$r<\log(c_2(M)/c)/(m-2n)\log p.$$

For a lattice $N_0\supset N$ which satisfies $d_p(N_0, M)\neq 0$ and $[N_0\colon N]=r$, there is an isometry σ from N_0 to M such that $\sigma(N_0)$ is primitive in M. Hence we have $[M\cap Q_p\sigma(N)\colon \sigma(N)]=[M\cap Q_p\sigma(N_0)\colon \sigma(N)]=[\sigma(N_0)\colon \sigma(N)]=[N_0\colon N]=p^r$ and have only to take $\sigma(N)$ as N' to complete the proof.

Next we will give a sufficient condition to the assumption of a) in Theorem 1.

Lemma 3. *Let M be a regular quadratic lattice over Z_p with* $\mathrm{rk}\,M=m\geqq 2n$, $\mathrm{ind}\,M\geqq n$. *Then there is a constant $c(M)$ such that for a regular submodule N of M with* $\mathrm{rk}\,N=n$, *there is a submodule N_0 of M which satisfies $N_0\cong N$ and $[M\cap Q_pN_0\colon N_0]<c(M)$.*

Proof. We use the induction on m. Take and fix a maximal sublattice $M'\subset M$ once and for all. Since $\mathrm{ind}\,M'=\mathrm{ind}\,M\geqq n$, M' is split by $\perp_n\left\langle p^a/2\begin{pmatrix}0&1\\1&0\end{pmatrix}\right\rangle$ for an integer a with $\mathfrak{n}(M')=p^aZ_p$, which represents primitively any regular quadratic lattice K of $\mathrm{rk}\,K=n$ with $\mathfrak{n}(K)\subset p^aZ_p$. Suppose $\mathfrak{n}(N)\subset p^aZ_p$ and take a primitive submodule N_0 of M' isometric to N. Noting the canonical injection from $M\cap Q_pN_0/N_0$ to M/M', we have $[M\cap Q_pN_0\colon N_0]\leqq[M\colon M']$. Next suppose $\mathfrak{n}(N)\supset p^aZ_p$, and decompose $N=N_1\perp N_2$ so that N_1 is modular and $\mathfrak{n}(N_1)\supset p^aZ_p$. Put $S=\{K\subset M\mid K\colon \text{modular}, \mathfrak{n}(K)\supset p^aZ_p\}$ and let $\{M_1, \cdots, M_r\}$ be representatives of $O(M)\backslash S$, and $\sigma(N_1)=M_i$ for some i and $\sigma\in O(M)$. If $N_2=0$, then $[M\cap Q_pN\colon N]\leqq\max_i[M\cap Q_pM_i\colon M_i]$. Suppose $N_2\neq 0$. We claim ind $M_i^\perp \geqq \mathrm{rk}\, N_2$. To do it, write $Q_pN_1 = \perp_{s_1} H \perp V$, $Q_pM_i^\perp = \perp_{s_2} H \perp W$, where H denotes the hyperbolic plane and V, W are anisotropic. Since $2s_1 + \dim V + \dim Q_pN_2 = \dim Q_pN_1 + \dim Q_pN_2 = n \leqq \mathrm{ind}\, M = \mathrm{ind}\,(Q_pM_i \perp Q_pM_i^\perp) = \mathrm{ind}\,(Q_pN_1 \perp Q_pM_i^\perp) = s_1 + s_2 + \mathrm{ind}\,(V \perp W)$, we have $\mathrm{ind}\, M_i^\perp - \mathrm{rk}\, N_2 = s_2 - \mathrm{rk}\, N_2 \geqq s_1 + \dim V - \mathrm{ind}\,(V \perp W) \geqq s_1 \geqq 0$. Applying the assumption of the induction to $\sigma(N_2) \subset M_i^\perp$, there is a constant $c(M_i^\perp)$ such that there is a submodule N_2' of $M_i^\perp$ isometric to $\sigma(N_2)$ with $[M_i^\perp \cap Q_pN_2' : N_2'] < c(M_i^\perp)$. Putting $N_0 = M_i \perp N_2'$, we have $N_0 \cong N_1 \perp N_2' \cong N$ and

$$\begin{aligned}[M \cap Q_pN_0 : N_0] &= [M \cap Q_pN_0 : (M_i \perp M_i^\perp) \cap Q_pN_0][(M_i \perp M_i^\perp) \cap Q_pN_0 : N_0] \\ &\leqq [M : M_i \perp M_i^\perp][M_i \perp (M_i^\perp \cap Q_pN_2') : M_i \perp N_2'] \\ &\leqq [M : M_i \perp M_i^\perp][M_i^\perp \cap Q_pN_2' : N_2'] \\ &< c(M_i^\perp)[M : M_i \perp M_i^\perp].\end{aligned}$$

Hence we have only to put $c(M) = \max([M : M'], [M \cap Q_pM_i : M_i], c(M_i^\perp)[M : M_i \perp M_i^\perp])$. The first step of the induction is the case when $\mathrm{rk}\, M = 2$ and M is isotropic, but the assertion is clear by the above argument in this case.

Theorem 2. *Let $0 \leqq r \leqq n \leqq m$ be integers and M, N_1 regular quadratic lattices over Z_p with $\mathrm{rk}\, M = m$, $\mathrm{rk}\, N_1 = r$ where $N_1 = 0$ if $r = 0$. Moreover we assume that there is a quadratic space V such that $Q_pM \cong Q_pN_1 \perp V$ and* ind *$V \geqq n - r$. Then there is a constant $c = c(M, N_1, n, r)$ such that if $N = N_1 \perp N_2$ is a regular quadratic lattice of* rk *$N = n$ represented by M, then there is a submodule $N_0 \subset M$ isometric to N with $[M \cap Q_pN_0 : N_0] < c$.*

Proof. Put $S = \{K \subset M \mid K \cong N_1\}$ and let $\{M_1, \cdots, M_t\}$ be representatives of $O(M) \backslash S$. Suppose that $N = N_1 \perp N_2$ is a regular lattice of $\mathrm{rk}\, N = n$ represented by M; then there is an isometry σ from N to M satisfying $\sigma(N_1) = M_i$ for some i. Since $N_1 \cong M_i$, $V \cong Q_pM_i^\perp$ and ind $Q_pM_i^\perp \geqq n - r = \mathrm{rk}\, N_2$. From Lemma 3 follows that there is a submodule N_2' of $M_i^\perp$ isometric to N_2 with $[M_i^\perp \cap Q_pN_2' : N_2'] < c(M_i^\perp)$ where $c(M_i^\perp)$ is a constant dependent only on $M_i^\perp$. Putting $N_0 = M_i \perp N_2'$, we have $N_0 \cong N$ and

$$\begin{aligned}[M \cap Q_pN_0 : N_0] = [M \cap Q_pN_0 &: (M_i \perp M_i^\perp) \cap Q_pN_0] \\ &\times [(M_i \perp M_i^\perp) \cap Q_p(M_i \perp N_2') : M_i \perp N_2'] \\ &\leqq [M : M_i \perp M_i^\perp][M_i^\perp \cap Q_pN_2' : N_2'] \\ &\leqq \max_i [M : M_i \perp M_i^\perp] c(M_i^\perp),\end{aligned}$$

which is to be denoted by $c(M, N_1, n, r)$.

Remark. Without assumption $\operatorname{ind} V \geqq n-r$, Theorem 2 does not hold. Since for a regular quadratic space U over $\boldsymbol{Q}_p$ we have $\operatorname{ind} U \geqq n$ if $\dim U \geqq 2n+3$, $m+r \geqq 2n+3$ is a sufficient condition to $\operatorname{ind} V \geqq n-r$. Hence we have $\alpha_p(N, M) > \kappa (>0)$ for some κ if $\operatorname{rk} M \geqq 2 \operatorname{rk} N+3$ and $\alpha_p(N, M) \neq 0$, taking $r=0$.

§ 3.

In this section we study the behaviour of $\alpha_p(p^r N, M)$ as $r \to \infty$.

Lemma 4. *Let M be a regular quadratic lattice over $\boldsymbol{Z}_p$ of* $\operatorname{ind} M = r$. *Then there are constants c_1, c_2 dependent only on M satisfying the following: Let $N = N_1 \perp N_2$ be a regular quadratic submodule of M with* $\operatorname{rk} N_1 = r$ *and suppose that the scale of any Jordan component of N_1 contains $\mathfrak{s}(N_2)$. If, then $\mathfrak{s}(N) \subset p^{c_1}\boldsymbol{Z}_p$, then there is an isometry σ from N to M such that $[M \cap \boldsymbol{Q}_p \sigma(N_1) \colon \sigma(N_1)] \leqq c_2$.*

Proof. We take and fix any maximal sublattice $M' = M_0 \perp M_1$ of M once and for all, where $\mathfrak{n}(M_0) = p^a \boldsymbol{Z}_p$, $\operatorname{ind} M_0 = r$, $\operatorname{rk} M_0 = 2r$ and M_1 is anisotropic. Let c_1 be an integer such that $c_1 \geqq a+4$ and $p^{4-c_1}\boldsymbol{Z}_p \supset \mathfrak{s}(M_1^\#)$. Suppose $\mathfrak{s}(N) \subset p^{c_1}\boldsymbol{Z}_p$; then $\mathfrak{n}(p^{-2}N_1) \subset \mathfrak{s}(p^{-2}N_1) = \mathfrak{s}(p^{-2}N) \subset p^{c_1-4}\boldsymbol{Z}_p \subset \mathfrak{n}(M_0)$ implies that there is a primitive submodule N_1' of M_0 isometric to $p^{-2}N_1$ and $N_1'^{\perp}$ in M_0 is isometric to $(N_1')^{(-1)}$ (the scaling of N_1' by -1). Since $\mathfrak{n}((N_1'^{\perp} \perp M_1)^\#) \subset \mathfrak{s}((N_1'^{\perp} \perp M_1)^\#) = \mathfrak{s}(N_1'^{\perp\#} \perp M_1^\#) = \mathfrak{s}((p^{-2}N_1)^\#) + \mathfrak{s}(M_1^\#) \subset p^4\mathfrak{s}(N_1^\#)$ follows from $p^4\mathfrak{s}(N_1^\#) \supset p^4\mathfrak{s}(N_1)^{-1} \supset p^{4-c_1}\boldsymbol{Z}_p \supset \mathfrak{s}(M_1^\#)$, we can take a $p^4\mathfrak{s}(N_1^\#)$-maximal lattice $\tilde{M}$ on $\boldsymbol{Q}_p(N_1'^{\perp} \perp M_1)$ containing $(N_1'^{\perp} \perp M_1)^\#$, and then $N_1'^{\perp} \perp M_1 \supset \tilde{M}^\#$. Decompose $\tilde{M}$ as $\tilde{M}_0 \perp \tilde{M}_1$ where $\operatorname{rk} \tilde{M}_0 = 2 \operatorname{ind} \tilde{M}_0$ and $\tilde{M}_1$ is anisotropic, and then $\tilde{M}_0^\#$ is a $4p^{-4}\mathfrak{s}(N_1^\#)^{-1}$-maximal lattice. Putting $\tilde{M}_1 = p^b K$ where K is $\boldsymbol{Z}_p$ or $p\boldsymbol{Z}_p$-maximal, we have $\tilde{M}_1^\# = p^{-b}K^\# \supset p^{-b}K$. Since $\mathfrak{n}(p^{-b}K) = p^{-2b}\mathfrak{n}(K) = \mathfrak{n}(K)^2\mathfrak{n}(\tilde{M}_1)^{-1} \supset \mathfrak{n}(K)^2 p^{-4}\mathfrak{s}(N_1^\#)^{-1} \supset \mathfrak{s}(N_1^\#)^{-1}$, $\tilde{M}_1^\#$ contains an $\mathfrak{s}(N_1^\#)^{-1}$-maximal lattice. Thus $\tilde{M}^\#$ contains an $\mathfrak{s}(N_1^\#)^{-1}$-maximal lattice since $\tilde{M}_0^\#$, $\tilde{M}_1^\#$ do. Since $\boldsymbol{Q}_p N_1 \perp \boldsymbol{Q}_p N_2 = \boldsymbol{Q}_p N \subset \boldsymbol{Q}_p M = \boldsymbol{Q}_p N_1' \perp \boldsymbol{Q}_p(N_1'^{\perp}$ in $M_0) \perp \boldsymbol{Q}_p M_1$ implies that $\boldsymbol{Q}_p N_2$ is represented by $\boldsymbol{Q}_p(N_1'^{\perp}$ in $M_0) \perp \boldsymbol{Q}_p M_1 \cong \boldsymbol{Q}_p \tilde{M}^\#$, and $\mathfrak{n}(N_2) \subset \mathfrak{s}(N_2) \subset \mathfrak{s}(N_1^\#)^{-1}$, there is a submodule N'' of $\tilde{M}^\#$ isometric to N_2. Defining an isometry σ from N to M by $\sigma(N_1) = p^2 N_1'$ and $\sigma(N_2) = N''$, we have

$$\begin{aligned}[M \cap \boldsymbol{Q}_p\sigma(N_1) \colon \sigma(N_1)] &= [M \cap \boldsymbol{Q}_p N_1' \colon p^2 N_1'] \\ &= [M \cap \boldsymbol{Q}_p N_1' \colon M' \cap \boldsymbol{Q}_p N_1'][M' \cap \boldsymbol{Q}_p N_1' \colon p^2 N_1'] \\ &\leqq [M \colon M'][N_1' \colon p^2 N_1'] \\ &= p^{2r}[M \colon M']\end{aligned}$$

which is to be c_2.

Lemma 5. *Let M, N be a regular quadratic lattice over Z_p and its regular submodule with* $\operatorname{rk} M=m$, $\operatorname{rk} N=n$. *Suppose that $n+1\leqq m$, $r=\operatorname{ind} M$, $N=N_1\perp N_2$ with $\operatorname{rk} N_1=r$ and that there is an isometry σ from N to M such that $[M\cap Q_p\sigma(N_1): \sigma(N_1)]<c$. Then we have $\alpha_p(N, M)>c_1\alpha_p(N_2, (\sigma(N_1)^{\perp} \text{ in } K)\perp(K^{\perp} \text{ in } M))\neq 0$ if $\mathfrak{s}(N)\subset p^{c_2}Z_p$. Here K is a primitive submodule of M such that $\operatorname{rk} K=2r$, $K\supset\sigma(N_1)$ and $\operatorname{ord} dK\leqq c_3$, and c is any gvien positive number and c_1, c_2, c_3 are positive numbers dependent only on M, c.*

Proof. We may assume $\mathfrak{n}(M)\subset 2Z_p$. For $N'=\sigma^{-1}(M\cap Q_p\sigma(N_1))\perp N_2(\supset N)$ we have

$$\begin{aligned}\alpha_p(N, M)&\geqq[N': N]^{n+1-m}\alpha_p(N', M) \qquad\qquad \text{(Proposition 4)}\\ &\geqq[N': N]^{n+1-m}\alpha_p(M\cap Q_p\sigma(N_1), M; M\cap Q_p\sigma(N_1))\\ &\quad\times\alpha_p(N_2, \sigma(N_1)^{\perp})\neq 0 \qquad\qquad \text{(Proposition 3).}\end{aligned}$$

Now we claim that there is a positive constant c_4 (and also $c_5, \cdots$, hereafter) dependent only on c, M such that $\alpha_p(M\cap Q_p\sigma(N_1), M; M\cap Q_p\sigma(N_1))>c_4$. Putting $L=M\cap Q_p\sigma(N_1)=Z_p[w_1, \cdots, w_r]$, we have

$$\begin{aligned}\alpha_p(L, M; L)=&[M^{\#}: M]^r\lim_{t\to\infty}(p^t)^{r(r+1)/2-mr}\#\{\sigma: L\longrightarrow M/p^tM^{\#}\,|\,B(\sigma x, \sigma y)\equiv\\ &B(x, y) \bmod p^tZ_p \text{ for } x, y\in L \text{ and } \eta(L)=Z_p[\sigma(w_1), \cdots,\\ &\sigma(w_r)] \text{ for some } \eta\in O(M)\}.\\ \geqq&[M^{\#}: M]^r\lim_{t\to\infty}(p^t)^{r(r+1)/2-mr}\#\{\sigma\in D_{p^t}(L, M)\,|\,\eta(L)=Z_p[\sigma(w_1),\\ &\cdots, \sigma(w_r)] \text{ for some } \eta\in O(M)\},\end{aligned}$$

where $\sigma(w_i)$ is an appropriate representative in M

$$\geqq[M^{\#}: M]^r\lim_{t\to\infty}(p^t)^{r(r+1)/2-mr}\#\left\{\sigma\in D_{p^t}(L, M)\,\middle|\,\begin{matrix}\sigma x\equiv x \bmod p^hM^{\#}\\ \text{for } x\in L\end{matrix}\right\}$$

where h is an integer such that $p^h\mathfrak{n}(M^{\#})\subset 2pZ_p$, since for $t\geqq h$ and $\sigma\in D_{p^t}(L, M)$, there is an isometry σ' from L to M such that $\sigma\equiv\sigma' \bmod p^tM^{\#}$ and by Corollary 2 on p. 182 in [6] σ' extends to an isometry η of M if $\sigma'(x)\equiv x \bmod p^hM^{\#}$ for $x\in L$, and thus $\eta L=Z_p[\sigma'(w_1), \cdots, \sigma'(w_r)]$. The last sequence is constant for $t\geqq h$. Hence $\alpha_p(L, M; L)\geqq[M^{\#}: M]^r\cdot(p^h)^{r(r+1)/2-mr}$. Thus we have $\alpha_p(M\cap Q_p\sigma(N_1), M; M\cap Q_p\sigma(N_1))>c_4$. It is easy to see $[N': N]<c$ and thus we have

$$\alpha_p(N, M)\geqq c^{n+1-m}c_4\alpha_p(N_2, \sigma(N_1)^{\perp})=c_5\alpha_p(N_2, \sigma(N_1)^{\perp}) \quad (\neq 0).$$

By virtue of Lemma 1 in Section 3 in [8] there is a submodule K of M such that $K\supset\sigma(N_1)$, $\mathrm{rk}\,K=2r$ and $\mathrm{ord}\,dK\leqq c_6$. Here we may suppose that K is primitive in M. We will show that for any isometry η from N_2 to $\sigma(N_1)^\perp$, $\eta(N_2)$ is contained in $(\sigma(N_1)^\perp$ in $K)\perp(K^\perp$ in $M)$. To do it, we have only to show that $x\in\sigma(N_1)^\perp$ with $Q(x)\in\mathfrak{s}(N)$ is in $(\sigma(N_1)^\perp$ in $K)\perp(K^\perp$ in $M)$ if $\mathfrak{s}(N)\subset p^{c_2}\boldsymbol{Z}_p$ for a sufficiently large c_2. Since $[M\colon K\perp K^\perp]\cdot\sigma(N_1^\perp)\subset\sigma(N_1)^\perp\cap(K\perp K^\perp)=(\sigma(N_1)^\perp$ in $K)\perp K^\perp$, there are $y\in\sigma(N_1)^\perp$ in K, $z\in K^\perp$ such that $[M\colon K\perp K^\perp]x=y+z$. First we note that the number of the isometry classes of K, $K^\perp$ is finite since $\mathrm{ord}\,dK\leqq c_6$. Suppose $\mathfrak{s}(N)\subset p^{4c_7}\boldsymbol{Z}_p$, where c_7 will be fixed in process of the proof. Since $K\supset\sigma(N_1)$, $\mathfrak{s}(\sigma(N_1))\subset p^{4c_7}\boldsymbol{Z}_p$ and $\mathrm{ord}\,dK\leqq c_6$, we can take c_7 so that $\mathrm{ind}\,K=r$. For a $\boldsymbol{Z}_p$-maximal lattice $\tilde{K}$ containing K we have $\mathrm{ord}\,[\tilde{K}\colon K]\leqq c_6/2$ and $[\tilde{K}\cap\boldsymbol{Q}_p\sigma(N_1)\colon\sigma(N_1)]=[\tilde{K}\cap\boldsymbol{Q}_p\sigma(N_1)\colon K\cap\boldsymbol{Q}_p\sigma(N_1)]\cdot[K\cap\boldsymbol{Q}_p\sigma(N_1)\colon\sigma(N_1)]\leqq[\tilde{K}\colon K][M\cap\boldsymbol{Q}_p\sigma(N_1)\colon\sigma(N_1)]<cp^{c_6/2}$. Putting $N_1'=\tilde{K}\cap\boldsymbol{Q}_p\sigma(N_1)$, we have $N_1'^\perp$ in $\tilde{K}\cong N_1'^{(-1)}$ and $[N_1'\colon\sigma(N_1)]<cp^{c_6/2}$, and hence $\mathfrak{s}(N_1')\subset p^{3c_7}\boldsymbol{Z}_p$ holds for a sufficiently large c_7 since $\mathfrak{s}(N_1)\subset\mathfrak{s}(N)\subset p^{4c_7}\boldsymbol{Z}_p$. From $y\in\sigma(N_1)^\perp$ in $K\subset\sigma(N_1)^\perp$ in $\tilde{K}=N_1'^\perp\cong N_1'^{(-1)}$, $Q(y)\in p^{3c_7}\boldsymbol{Z}_p$ follows. Then $[M\colon K\perp K^\perp]^2Q(x)=Q(y)+Q(z)$ implies $Q(z)\in p^{3c_7}\boldsymbol{Z}_p$. Since $K^\perp$ is anisotropic and $\mathrm{ord}\,dK^\perp\leqq c_8$, we can take c_7 so that $[M\colon K\perp K^\perp]^{-1}z\in K^\perp$, and hence $[M\colon K\perp K^\perp]^{-1}y=x-[M\colon K\perp K^\perp]^{-1}z\in\boldsymbol{Q}_p(\sigma(N_1)^\perp$ in $K)\cap M=\sigma(N_1)^\perp$ in K. Thus we have proved $x\in\sigma(N_1)^\perp$ in $K\perp K^\perp$, and then by virtue of Proposition 4, $\alpha_p(N,M)\geqq c_5\alpha_p(N_2,\sigma(N_1)^\perp)=c_5[\sigma(N_1)^\perp\colon(\sigma(N_1)^\perp$ in $K)\perp K^\perp]^{-(n-r)}\cdot\alpha_p(N_2,(\sigma(N_1)^\perp$ in $K)\perp K^\perp)\neq 0$. Since $[M\colon K\perp K^\perp]\cdot\sigma(N_1)^\perp\subset\sigma(N_1)^\perp\cap(K\perp K^\perp)=(\sigma(N_1)^\perp$ in $K)\perp K^\perp$, we have $[\sigma(N_1)^\perp\colon(\sigma(N_1)^\perp$ in $K)\perp K^\perp]\leqq[M\colon K\perp K^\perp]^{m-r}$ and hence $\alpha_p(N,M)\geqq c_5[M\colon K\perp K^\perp]^{(m-r)(r-n)}\cdot\alpha_p(N_2,(\sigma(N_1)^\perp$ in $K)\perp K^\perp)\neq 0$. This completes the proof.

Lemma 6. *We keep everything in Lemma 5. There is a positive constant c' dependent only on M such that x in $(\sigma(N_1)^\perp$ in $K)\perp K^\perp$ with $Q(x)\in\mathfrak{s}(N)$ is contained in $(\sigma(N_1)^\perp$ in $K)\perp p^{[a/2]-c'}K^\perp$ where a is defined by $\mathfrak{s}(N)=p^a\boldsymbol{Z}_p$.*

Proof. We may assume $\mathfrak{n}(M)\subset 2\boldsymbol{Z}_p$ and use notations in the proof of the previous lemma. Let x be an element of $(\sigma(N_1)^\perp$ in $K)\perp K^\perp$ with $Q(x)\in\mathfrak{s}(N)$, and write $x=y+z$ with $y\in\sigma(N_1)^\perp$ in K, $z\in K^\perp$. Since $y\in\sigma(N_1)^\perp$ in $K\subset\sigma(N_1)^\perp$ in $\tilde{K}=N_1'^\perp$ in $\tilde{K}\cong N_1'^{(-1)}$ and $d=[N_1'\colon\sigma(N_1)]<cp^{c_6/2}$, we have $Q(y)\in\mathfrak{n}(N_1')\subset\mathfrak{n}(d^{-1}\sigma(N_1))\subset d^{-2}p^a\boldsymbol{Z}_p$ and hence $Q(z)=Q(x)-Q(y)\in d^{-2}p^a\boldsymbol{Z}_p$. Take a p^{c_9}-maximal sublattice K' of $K^\perp$, and then we have $Q(p^{c_9-[a/2]}dz)=p^{2c_9-2[a/2]}d^2Q(z)\subset p^{2c_9}\boldsymbol{Z}_p$. Hence $p^{c_9-[a/2]}dz$ is contained in K' since $\boldsymbol{Q}_pK'=\boldsymbol{Q}_pK^\perp$ is anisotropic. Thus z is in $p^{[a/2]-c_9}d^{-1}K'\subset p^{[a/2]-c'}K^\perp$ for some positive constant c' depending only on c, c_9, c_6.

Theorem 3. *Let M, N be regular quadratic lattices over $\boldsymbol{Z}_p$ with* $\mathrm{rk}\, M=m$, $\mathrm{rk}\, N=n$ *satisfying $n+1\leqq m$. Assume that $N=N_1\perp N_2$ with* $\mathrm{rk}\, N_1=\mathrm{ind}\, M$ *($=r$, say) and there is an isometry σ from N to M such that* $[M\cap \boldsymbol{Q}_p\sigma(N_1): \sigma(N_1)]<c$ *for a given constant c. Then there are positive constants $c_1, \cdots, c_4$ depending only on M and c such that if* $\mathrm{ord}\, \mathfrak{s}(N)$ *($=a$, say)$\geqq c_1$, then* $\alpha_p(N, M)>c_2 p^{[a/2](n-r)(n+r+1-m)}\alpha_p(p^{-[a/2]}N_2, p^{-[a/2]}(\sigma(N_1)^\perp \text{ in } K)\perp p^{-c_3}K^\perp)\neq 0$, *where K is a primitive submodule of M such that $K\supset \sigma(N_1)$,* $\mathrm{rk}\, K=2r$, $\mathrm{ind}\, K=r$ *and* $\mathrm{ord}\, dK\leqq c_4$.

Proof. By virtue of the previous two lemmas and Proposition 4, we have

$$\begin{aligned}\alpha_p(N, M)&>c_5\alpha_p(N_2, (\sigma(N_1)^\perp \text{ in } K)\perp K^\perp)\\ &=c_5[(\sigma(N_1)^\perp \text{ in } K)\perp K^\perp: (\sigma(N_1)^\perp \text{ in } K)\perp p^{[a/2]-c'}K^\perp]^{-(n-r)}\\ &\quad\times\alpha_p(N_2, (\sigma(N_1)^\perp \text{ in } K)\perp p^{[a/2]-c'}K^\perp)\end{aligned}$$

where we assume that $a/2\geqq c'$ in Lemma 6,

$$\begin{aligned}&=c_5 p^{([a/2]-c')(m-2r)(r-n)+[a/2](n-r)(n-r+1)}\\ &\quad\times\alpha_p(p^{-[a/2]}N_2, p^{-[a/2]}(\sigma(N_1)^\perp \text{ in } K)\perp p^{-c'}K^\perp)\\ &=c_5 p^{c'(m-2r)(n-r)}\cdot p^{[a/2](n-r)(n+r+1-m)}\\ &\quad\times\alpha_p(p^{-[a/2]}N_2, p^{-[a/2]}(\sigma(N_1)^\perp \textit{ in } K)\perp p^{-c'}K^\perp).\end{aligned}$$

Remark. Lemma 4 gives a sufficient condition for the assumption in the theorem.

Corollary. *Let $M\supset N$ be regular quadratic lattices with* $\mathrm{rk}\, M=m$, $\mathrm{rk}\, N=n\geqq \mathrm{ind}\, M=r$, *and suppose $n+1\leqq m$. Then there is a positive constant $c(M, N)$ such that $\alpha_p(p^tN, M)>c(M, N)p^{t(n-r)(n+r+1-m)}$ for $t\geqq 0$.*

Proof. There is a lattice N' which contains N and is an orthogonal sum of one-dimensional lattices and $[N': N]$ is less than a number depending only on n. From Proposition 4 follows $\alpha_p(p^tN, M)\geqq [N': N]^{n+1-m}\alpha_p(p^tN', M)$. $M\supset N$ implies $p^tN'\subset M$ for t with $p^t\geqq [N': N]$. Write $N'=N_1\perp N_2$ where $\mathrm{rk}\, N_1=r$ and the scale of any Jordan component of N_1 contains $\mathfrak{s}(N_2)$. By virtue of Lemma 4, there is an isometry σ from p^tN' to M such that $[M\cap \boldsymbol{Q}_p\sigma(p^tN_1): \sigma(p^tN_1)]\leqq p^{c_2}$ if $\mathfrak{s}(p^tN')\subset p^{c_1}\boldsymbol{Z}_p$ and $p^t\geqq [N': N]$ for c_1, c_2 in it. From the theorem $\alpha_p(p^tN', M)> cp^{[a/2](n-r)(n+r+1-m)}\alpha_p(p^{t-[a/2]}N_2, p^{-[a/2]}(\sigma(p^tN_1)^\perp \text{ in } K)\perp p^{-c_3}K^\perp)$ if $a=\mathrm{ord}\, \mathfrak{s}(p^tN')$ is sufficiently large, where K is a primitive submodule of M such that $K\supset\sigma(p^tN_1)$, $\mathrm{rk}\, K=2r$, $\mathrm{ind}\, K=r$ and $\mathrm{ord}\, dK\leqq c_4$ and c, c_3, c_4 depend only on M. Since N, N', N_1, N_2, are fixed, $|a-2t|$ is bounded and hence $p^{t-[a/2]}N_2$ can run over only a finite number of isometry classes. Let $\tilde{K}$ be a maximal $\boldsymbol{Z}_p$ lattice containing K: then $[\tilde{K}: K] \leqq p^{c_4/2}$ and $M \cap \boldsymbol{Q}_p\sigma(p^tN_1) = K \cap \boldsymbol{Q}_p\sigma(p^tN_1)$ is contained in $\tilde{K} \cap \boldsymbol{Q}_p\sigma(p^tN_1)$ with index$\leqq [\tilde{K}: K]$. Noting that $\sigma(p^tN_1)^\perp$ in $\tilde{K}$ is isometric to $(\tilde{K} \cap \boldsymbol{Q}_p\sigma(p^tN_1))^{(-1)}$, we have $(p^{-c_2}[\tilde{K}: K]^{-1}\sigma(p^tN_1))^{(-1)} \supset (\tilde{K} \cap \boldsymbol{Q}_p(\sigma(p^tN_1)))^{(-1)} \cong \sigma(p^tN_1)^\perp$ in $\tilde{K} \supset \sigma(p^tN_1)^\perp$ in $K \supset [\tilde{K}: K](\sigma(p^tN_1)^\perp$ in $\tilde{K}) \cong [\tilde{K}: K](\tilde{K} \cap \boldsymbol{Q}_p(\sigma(p^tN_1)))^{(-1)} \supset [\tilde{K}: K]\sigma(p^tN_1)^{(-1)}$ and hence $p^{t-[a/2]}[\tilde{K}: K]N_1^{(-1)} \hookrightarrow p^{-[a/2]}(\sigma(p^tN_1)^\perp$ in $K) \hookrightarrow p^{t-[a/2]-c_2}[\tilde{K}: K]^{-1}N_1^{(-1)}$. Thus $p^{-[a/2]}(\sigma(p^tN_1)^\perp$ in $K)$ runs over a finite number of isometry classes depending only on M, N, and hence we have $\alpha_p(p^{t-[a/2]}N_2,\ p^{-[a/2]}(\sigma(p^tN_1)^\perp$ in $K) \perp p^{-c_3}K^\perp) \geqq c_5$ (>0) where c_5 depends only on M, N. Therefore we have proved the theorem.

Remark. For integers $0 \leqq r \leqq n \leqq m$ with $n+1 \leqq m \leqq 2n$, $0 \leqq m-2r \leqq 4$ it is easy to see $(n-r)(n+r+1-m)<0$ if and only if $n=r+2$ and $m-2r=4$. Unless, hence $\operatorname{rk} M - 2\operatorname{ind} M = 4$, $\operatorname{rk} N = \operatorname{ind} M + 2$, there is a positive constant c such that $\alpha_p(p^tN, M) > c$ if $\alpha_p(N, M) \neq 0$.

§ 4.

In this section we show that $\alpha_p(p^tN, M)$ seems to tend to zero as $t \to \infty$ in the exceptional case in the last remark.

We assume that p is an odd prime in this section. We will prove

Theorem 4. *Let M be a quadratic lattice $\underset{r}{\perp}\left\langle\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\right\rangle \perp \langle 1\rangle \perp \langle -\delta\rangle \perp \langle p\rangle \perp \langle -\delta p\rangle$ where δ is a non-square unit. For a regular quadratic lattice N over $\boldsymbol{Z}_p$ with* $\operatorname{rk} N = n \leqq \operatorname{rk} M$ *we consider the formal power series*

$$f(x) = \sum_{t=0}^{\infty} \alpha_p(N^{(p^t)}, M)x^t.$$

Then $f(x)$ is a rational function in x whose denominator is

$$\prod_{0 \leqq j \leqq n} (1 - p^{(n-j)(n+j+1-2r-4)/2}x).$$

Remark. If $n=r+2$, then the denominator of $f(x)$ seems to become

$$\prod_{0 \leqq j \leqq n-2} (1 - p^{(n-j)(n+j+1-2r-4)/2}x) = \prod_{0 \leqq j \leqq n-2} (1 - p^{(n-j)(j+1-n)/2}x)$$
$$= \prod_{2 \leqq j \leqq n} (1 - p^{-j(j-1)/2}x),$$

and this is the case at least $n \leqq 9$. If this is the case, $f(x)$ converges for $|x| < p$ and so $\alpha_p(N^{(p^t)}, M)(p^{1-\varepsilon})^t < c$ for any positive number ε and some constant c. Hence we have $\alpha_p(p^tN, M)<c(p^\varepsilon)^{2t}p^{-2t}$. Let M' be a regular quadratic lattice over Z_p with $\operatorname{rk} M'-2\operatorname{ind} M'=4$ and $n=\operatorname{rk} N=\operatorname{ind} M'+2$, and M a Z_p-maximal lattice containing M'. Then we have

$$\begin{aligned} c(M', N)p^{-2t} &< \alpha_p(p^tN, M') && \text{(Corollary in § 3)} \\ &\leqq [M: M']^n \alpha_p(p^tN, M) && \text{(Proposition 4)} \\ &\leqq c[M: M']^n (p^\varepsilon)^{2t} p^{-2t}. \end{aligned}$$

Hence in the exceptional case in the last remark $\alpha_p(p^tN, M')$ tends to zero under the reduction of the denominator of $f(x)$. Is the estimate of $\alpha_p(N, M)$ from below in Theorem 3 and the corollary almost best?

We need several lemmas to prove the theorem.

Put $S=S_r=\operatorname{diag}\Big(\underbrace{\begin{pmatrix}0&1\\1&0\end{pmatrix}, \cdots, \begin{pmatrix}0&1\\1&0\end{pmatrix}}_{r}, 1, -\delta, p, -\delta p\Big)$ where δ is a nonsquare unit, and denote by $\mathfrak{S}_n$ the set of all integral symmetric matrices of size n with entries in Z_p.

Lemma 7. *For non-negative integers $a\leqq t$, we have for any $\varepsilon \in Z_p^\times$*

$$\sum_{g\in Z_p^{2r+4} \bmod p^t} e(S[g]\varepsilon p^a/p^t)=\begin{cases} -p^{(r+2)(t+a)+1} & \text{if } a<t, \\ p^{(r+2)(t+a)} & \text{if } a=t, \end{cases}$$

where $e(x)=\exp(2\pi i x)$.

Proof. For $a=t$, the lemma is obvious. We suppose $a<t$. Since

$$\begin{aligned} &\sum_g e(S[g]\varepsilon p^a/p^t) \\ &=\{\sum_{x,y \bmod p^t} e(2xy\varepsilon p^{a-t})\}^r (\sum_{x \bmod p^t} e(x^2\varepsilon p^{a-t}))(\sum_{x \bmod p^t} e(-x^2\delta\varepsilon p^{a-t})) \\ &\quad\times(\sum_{x \bmod p^t} e(x^2\varepsilon p^{a+1-t}))(\sum_{x \bmod p^t} e(-x^2\delta\varepsilon p^{a+1-t})) \end{aligned}$$

and

$$\begin{aligned} \sum_{x,y \bmod p^t} e(2xy\varepsilon p^{a-t}) &= p^t \,\#\{x \bmod p^t \mid x\equiv 0 \bmod p^{t-a}\} \\ &= p^{t+a}, \end{aligned}$$

$$\sum_{x \bmod p^t} e(x^2\varepsilon p^{a-t}) = p^{(t+a)/2}\left(\frac{\varepsilon}{p}\right)^{t-a} \begin{cases} 1 & \text{if } p^{t-a}\equiv 1 \bmod 4, \\ \sqrt{-1} & \text{otherwise}, \end{cases}$$

we have

$$\sum_{g} e(S[g]\varepsilon p^a/p^t)$$
$$= p^{r(t+a)} p^{(t+a)/2} \left(\frac{\varepsilon}{p}\right)^{t-a} p^{(t+a)/2} \left(\frac{-\delta\varepsilon}{p}\right)^{t-a} \left(\frac{-1}{p}\right)^{t-a}$$
$$\times p^{(t+a+1)/2} \left(\frac{\varepsilon}{p}\right)^{t-a-1} p^{(t+a+1)/2} \left(\frac{-\delta\varepsilon}{p}\right)^{t-a-1} \left(\frac{-1}{p}\right)^{t-a-1}$$
$$= -p^{(r+2)(t+a)+1}.$$

We put

$$\alpha'_p(T, S) = 2^{\delta_{m,n}} \alpha_p(T, S)$$
$$= \lim_{t\to\infty} (p^t)^{n(n+1)/2-mn} \# \{G \in M_{m,n}(\boldsymbol{Z}_p) \bmod p^t \mid S[G] \equiv T \bmod p^t\},$$

where T is a regular matrix in $\mathfrak{S}_n$ and $m = 2r+4$. We denote by $\boldsymbol{Q}_p\mathfrak{S}_n$ the set of all symmetric matrices of size n with entries in $\boldsymbol{Q}_p$. For $R \in \boldsymbol{Q}_p\mathfrak{S}_n$, let $\{p^{a_1}, \cdots, p^{a_r}\}$ $(a_1 \leqq \cdots \leqq a_k < 0 \leqq a_{k+1} \leqq \cdots)$ be non-zero elementary divisors and put $w(R) = (-p)^k$ and $\nu(R) = p^{-\sum_{i=1}^k a_i}$, where $w(R) = \nu(R) = 1$ if all elementary divisors are integral.

Lemma 8. *$\alpha'_p(T, S) = \lim_{t\to\infty} \sum_{R \in \boldsymbol{Q}_p\mathfrak{S}_n/\mathfrak{S}_n,\ p^tR \in \mathfrak{S}_n} e(-\operatorname{tr} TR) w(R) \nu(R)^{-r-2}$ and if $r \geqq n$, then $\alpha'_p(T, S) = \sum_{R \in \boldsymbol{Q}_p\mathfrak{S}_n/\mathfrak{S}_n} e(-\operatorname{tr} TR) w(R) \nu(R)^{-r-2}$ is absolutely convergent.*

Proof. $\# \{G \in M_{m,n}(\boldsymbol{Z}_p) \bmod p^t \mid S[G] \equiv T \bmod p^t\}$
$$= p^{-tn(n+1)/2} \sum_{G \bmod p^t} \sum_{X \in \mathfrak{S}_n/p^t\mathfrak{S}_n} e(\operatorname{tr}((S[G]-T)X)p^{-t})$$
$$= p^{-tn(n+1)/2} \sum_{X \in \mathfrak{S}_n/p^t\mathfrak{S}_n} e(-\operatorname{tr}(TX)p^{-t}) \sum_{G} e(\operatorname{tr}(S[G]X)p^{-t}).$$

Here we put $X = \operatorname{diag}(\varepsilon_1 p^{a_1}, \cdots, \varepsilon_n p^{a_n})[U]$, $U \in GL_n(\boldsymbol{Z}_p)$ and may assume $\varepsilon_i \in \boldsymbol{Z}_p^\times$, $0 \leqq a_1 \leqq \cdots \leqq a_n \leqq t$; then we have

$$\sum_{G} e(\operatorname{tr}(S[G]X)p^{-t})$$
$$= \prod_{i=1}^{n} \Big(\sum_{g \bmod p^t} e(S[g]\varepsilon_i p^{a_i - t}) \Big)$$
$$= p^{(r+2)\sum_{i=1}^n (t+a_i)} w(p^{-t}X)$$
$$= p^{2(r+2)tn} \nu(p^{-t}X)^{-(r+2)} w(p^{-t}X),$$

and this gives the first expression of $\alpha'_p(T, S)$. The second follows from usual arguments.

Let C, D be matrices in $M_n(Z_p)$ and write $(C, D)=1$ if C^tD is symmetric and all elementary divisors of $n\times 2n$ matirx (C, D) are 1. Let $\{p^{\lambda_1}, \cdots, p^{\lambda_n}\}$ be elementary divisors of $C(|C|\neq 0)$ and put $\chi=\mathrm{diag}(p^{\lambda_1}, \cdots, p^{\lambda_n})$, $C=V\chi U$, $U, V \in GL_n(Z_p)$ and $D=VD'{}^tU^{-1}$; then $C^{-1}D=(\chi^{-1}D')[{}^tU^{-1}]$ and its non-integral elementary divisors are $\{p^{-\lambda_i}\,|\,\lambda_i>0\}$ and we may suppose that U is uniquely determined as one of representatives of $(GL_n(Z_p)\cap\chi^{-1}GL_n(Z_p)\chi)\backslash GL_n(Z_p)$. It is easy to see that any element of $Q_p\mathfrak{S}_n$ can be expressed as $C^{-1}D$ with $(C, D)=1$. Hence the sum $\sum_R e(\mathrm{tr}\, TR)$ where R runs over $Q_p\mathfrak{S}_n/\mathfrak{S}_n$ so that the non-integral elementary divisors of R are $\{p^{-\lambda_i}\,|\,\lambda_i>0\}$ is equal to

$$\sum_{\substack{U\in(GL_n(Z_p)\cap\chi^{-1}GL_n(Z_p)\chi)\backslash GL_n(Z_p)\\ (\chi,D)=1\\ D\in M_n(Z)/\chi\mathfrak{S}_n}} e(\mathrm{tr}\,(\chi^{-1}D)[{}^tU^{-1}]\cdot T))$$

$$=\sum_U\sum_D e(\mathrm{tr}\, T[U^{-1}]\cdot\chi^{-1}D).$$

We put $\Lambda=\{(\lambda_1, \cdots, \lambda_n)\,|\,0\leqq\lambda_1\leqq\cdots\leqq\lambda_n,\ \lambda_i\in Z\}$ and for $\lambda=(\lambda_1, \cdots, \lambda_n)\in\Lambda$ we put $\chi(\lambda)=\mathrm{diag}(p^{\lambda_1}, \cdots, p^{\lambda_n})$ and

$$R_n(T, \lambda)=\sum_D e(\mathrm{tr}\, T\chi(\lambda)^{-1}D)$$

where D runs over $M_n(Z_p) \bmod \chi(\lambda)\mathfrak{S}_n$ so that $(\chi(\lambda), D)=1$, and put $w(\lambda)=(-p)^{n-k}$ if $\lambda_k=0<\lambda_{k+1}$. Now we have a new expression for $\alpha_p'(T, S)$

$$\alpha_p'(T, S)=\sum_{\lambda\in\Lambda} w(\lambda)p^{-(\Sigma\lambda_i)(r+2)}\sum_{U\in G_n(\lambda)} R_n(-T[U^{-1}], \lambda)$$

if $r\geqq n$, where we put $G_n(\lambda)=(GL_n(Z_p)\cap\chi(\lambda)^{-1}GL_n(Z_p)\chi(\lambda))\backslash GL_n(Z_p)$.

We define $\beta(s, T)$ by

$$\beta(s, T)=\sum_{\lambda\in\Lambda} w(\lambda)p^{-(\Sigma\lambda_i)s}\sum_{U\in G_n(\lambda)} R_n(T[U^{-1}], \lambda).$$

$\beta(s, T)$ is absolutely convergent if $s\geqq n+2$, and $\alpha_p'(T, S)=\beta(r+2, -T)$ if $r\geqq n$.

Lemma 9. *For a regular $T\in\mathfrak{S}_n$, $\beta(s, T)$ is a polynomial in p^{-s} and $\beta(r+2, -T)=\alpha_p'(T, S_r)$ if $2r+4\geqq n$.*

Proof. For a sufficiently large t, which is dependent not on r but on T,

$$\alpha_p'(T, S_r)=\sum_{\substack{R\in Q_p\mathfrak{S}_n/\mathfrak{S}_n\\ p^tR\in\mathfrak{S}_n}} e(-TR)w(R)\nu(R)^{-r-2}$$

$$=\beta(r+2, -T; t) \qquad \text{for } r\geqq n/2-2$$

where $\beta(s, T; t)$ is the partial sum on $\lambda=(\lambda_1, \cdots, \lambda_n) \in \Lambda$ with $\lambda_n \leqq t$. Since $\beta(s, T; t)$ and $\beta(s, T; t+1)$ are polynomials in p^{-s} and $\beta(r+2, T; t)=\beta(r+2, T; t+1)=\alpha'_p(-T, S_r)$ for $r \geqq n/2-2$, we have $\beta(s, T; t)=\beta(s, T; t+1)=\cdots=\beta(s, T)$. Hence it completes the proof.

Lemma 10. *For a natural number k, the number of symmetric regular matrices of size k with entries in Z/pZ is equal to* $p^{k(k+1)/2} \prod_{\substack{1 \leqq i \leqq k \\ odd}} (1-p^{-i})$.

Proof. A symmetric regular matrix with entries in $F=Z/pZ$ is equivalent to one of $S_1=\mathrm{diag}(1, \cdots, 1)$ or $S_2=\mathrm{diag}(1, \cdots, 1, \delta)$ where δ is a non-square. Thus the number in question is equal to

$$\frac{\# GL_k(F)}{\# O(S_1)}+\frac{\# GL_k(F)}{\# O(S_2)}.$$

It is known that $\# GL_k(F)=(p^k-1)(p^k-p)\cdots(p^k-p^{k-1})$, $\# O(S_1)=\# O(S_2)=2p^{k(k-1)/2} \prod_{1 \leqq i \leqq (k-1)/2} (1-p^{-2i})$ if k is odd, and $\# O(\mathrm{diag}(1, \cdots, 1, \eta))=2p^{k(k-1)/2}\left(1-\left(\frac{(-1)^{k/2}\eta}{p}\right)p^{-k/2}\right) \prod_{1 \leqq i \leqq k/2-1} (1-p^{-2i})$ for $\eta \in F^{\times}$ if k is even where (—) is the quadratic residue symbol. The lemma follows immediately from these.

For $0 \leqq k \leqq h \leqq n$ we put

$$\Lambda_k=\{\lambda=(\lambda_1, \cdots, \lambda_n) \in \Lambda \mid \lambda_i>0 \text{ if and only if } i>k\},$$
$$\Lambda_{k,h}=\{\lambda \in \Lambda_k \mid \lambda_i=1 \text{ if } k<i \leqq h,\ \lambda_i \geqq 2 \text{ if } i>h\}.$$

It is obvious that

$$\Lambda_0=\{\lambda \in \Lambda \mid \lambda_1 \geqq 1\},\ \Lambda_n=\{(0, \cdots, 0)\},$$
$$\Lambda_{k,k}=\{\lambda \in \Lambda \mid 0=\cdots=\lambda_k<\lambda_{k+1} \leqq \cdots,\ \lambda_{k+1} \geqq 2\}$$
$$\Lambda=\coprod_{0 \leqq k \leqq n} \Lambda_k,\ \Lambda_k=\coprod_{k \leqq h \leqq n} \Lambda_{k,h}.$$

Lemma 11. *For $T \in \mathfrak{S}_n$ and $\lambda \in \Lambda_{k,h}$ $(0 \leqq k \leqq h \leqq n)$, we have*

$$R_n(pT, \lambda)=p^{(n-k)(n-k+1)/2} \prod_{\substack{1 \leqq i \leqq h-k \\ i:odd}} (1-p^{-i}) R_n(T, \lambda-1),$$

where $\lambda-1=(0, \cdots, 0, \lambda_{k+1}-1, \cdots, \lambda_n-1) \in \Lambda_h$.

Proof. First we claim that for $\lambda \in \Lambda_k$, we have $R_n(T, \lambda)=R_{n-k}(T', (\lambda_{k+1}, \cdots, \lambda_n))$ where T' is the lower right $(n-k)\times(n-k)$ submatrix. For $P=\mathrm{diag}(p^{\lambda_{k+1}}, \cdots, p^{\lambda_n})$, $\chi(\lambda)=\begin{pmatrix} 1_k & \\ & P \end{pmatrix}$ holds and it is easy to see that $(\chi(\lambda), D)=1$ if and only if $D_1={}^tD_1$, $D_3=P{}^tD_2$, $(P, D_4)=1$ where $D=\begin{bmatrix} D_1^{(k)} & D_2 \\ D_3 & D_4 \end{bmatrix}$. Since $\chi(\lambda)\begin{bmatrix} S_1 & S_2 \\ {}^tS_2 & S_4 \end{bmatrix}=\begin{bmatrix} S_1 & S_2 \\ P{}^tS_2 & PS_4 \end{bmatrix}$, the representatives mod $\chi(\lambda)\mathfrak{S}_n$ of D which satisfies $(\chi(\lambda), D)=1$ can be chosen to be $\left\{\begin{bmatrix}0 & 0\\ 0 & D_4\end{bmatrix} \middle| (P, D_4)=1\ D_4 \bmod P\mathfrak{S}_{n-k}\right\}$, and then we have

$$R_n(T, \lambda)=\sum_{D_4} e\left(\operatorname{tr} T\begin{bmatrix}1_k & \\ & P^{-1}\end{bmatrix}\begin{bmatrix}0 & 0\\ 0 & D_4\end{bmatrix}\right)$$
$$=\sum_{D_4} e(\operatorname{tr} T'P^{-1}D_4)$$
$$=R_{n-k}(T', (\lambda_{k+1}, \cdots, \lambda_n)).$$

Suppose that $\lambda \in \Lambda_{0,0}$, i.e., $\lambda_1 \geqq 2$. It is easy to see that $(\chi(\lambda), D)=1$ holds if and only if

$\chi(\lambda)^{-1}D$ is symmetric and D is in $GL_n(\boldsymbol{Z}_p)$

$\Leftrightarrow \chi(\mu)^{-1}D$ is symmetric for $\mu=(\lambda_1-1, \cdots, \lambda_n-1)$

D is in $GL_n(\boldsymbol{Z}_p)$

$\Leftrightarrow (\chi(\mu), D)=1$

since $\chi(\lambda)=p\chi(\mu)\equiv 0 \bmod p^2$.

Putting $D=D_1+\chi(\mu)X$, D runs over the representatives mod $\chi(\lambda)\mathfrak{S}_n$ of D safisfying $(\chi(\lambda), D)=1$ if and only if D_1 runs over the representatives mod $\chi(\mu)\mathfrak{S}_n$ of D_1 satisfying $(\chi(\mu), D_1)=1$ and X runs over $\mathfrak{S}_n/p\mathfrak{S}_n$. Hence we have

$$R_n(pT, \lambda)=\sum_{\substack{D_1\\ X}} e(\operatorname{tr} pTp^{-1}\chi(\mu)^{-1}(D_1+\chi(\mu)X))$$
$$=\sum_{D_1} e(\operatorname{tr} T\chi(\mu)^{-1}D_1) \sum_X e(\operatorname{tr}(TX))$$
$$=p^{n(n+1)/2}R_n(T, \mu).$$

Suppose that $\lambda \in \Lambda_{0,h}$ $(h\geqq 1)$, i.e., $1=\lambda_1=\cdots=\lambda_h<\lambda_{h+1}\leqq\cdots$. Putting $\chi(\lambda)=\begin{bmatrix}p1_h & \\ & P\end{bmatrix}$, $D=\begin{bmatrix}D_1^{(h)} & D_2\\ D_3 & D_4\end{bmatrix}$, it is easy to see $(\chi(\lambda), D)=1$ if and only if $D_1={}^tD_1 \in GL_h(\boldsymbol{Z}_p)$, $D_3=p^{-1}P\,{}^tD_2$ and $(P, D_4)=1$. Hence we have

$$R_n(pT, \lambda)=\sum_{D_1, D_2, D_4} e\left(\operatorname{tr} pT\begin{bmatrix}p^{-1}1_h & \\ & P^{-1}\end{bmatrix}\begin{bmatrix}D_1 & D_2\\ p^{-1}P\,{}^tD_2 & D_4\end{bmatrix}\right),$$

where D_1, D_2 and D_4 run over $\{D_1 \in \mathfrak{S}_h/p\mathfrak{S}_h \mid |D_1|\not\equiv 0 \bmod p\}$, $D_2 \in M_{h,n-h}(Z/pZ)$ and $\{D_4 \in M_{n-h}(Z_p) \bmod P\mathfrak{S}_{n-h} \mid (P, D_4)=1\}$ respectively,

$$=\#\{D_1\}p^{h(n-h)}R_{n-h}(pT', (\lambda_{h+1}, \cdots, \lambda_n))$$

where T' is the right lower $(n-h)\times(n-h)$ submatrix of T,

$$=p^{h(h+1)/2}\prod_{\substack{1\leqq i\leqq h\\ i:odd}}(1-p^{-i})\cdot p^{h(n-h)}\cdot p^{(n-h)(n-h+1)/2}$$
$$\times R_{n-h}(T', (\lambda_{h+1}-1, \cdots, \lambda_n-1))$$
$$=p^{n(n+1)/2}\prod_{\substack{1\leqq i\leqq h\\ i:odd}}(1-p^{-i})R_n(T, \lambda-1).$$

Finally, for $\lambda \in \Lambda_{k,h}$, we have

$$R_n(pT, \lambda)=R_{n-k}(pT', (\lambda_{k+1}, \cdots, \lambda_n))$$

where T' is the right lower $(n-k)\times(n-k)$ submatrix of T

$$=p^{(n-k)(n-k+1)/2}\prod_{\substack{1\leqq i\leqq h-k\\ i:odd}}(1-p^{-i})\cdot R_{n-k}(T', (\lambda_{k+1}-1, \cdots, \lambda_n-1))$$
$$=p^{(n-k)(n-k+1)/2}\prod_{\substack{1\leqq i\leqq h-k\\ i:odd}}(1-p^{-i})\cdot R_n(T, \lambda-1).$$

We denote by $F(x)$, $F(x; k, h)$ $(0\leqq k\leqq h\leqq n)$

$$\sum_{t\geqq 0}\beta(s, p^tT)x^t, \quad \sum_{t\geqq 0}\Big(\sum_{\lambda\in\Lambda_{k,h}}w(\lambda)p^{-(\Sigma\lambda_i)s}\sum_{U\in G_n(\lambda)}R_n(p^tT[U^{-1}], \lambda)\Big)x^t$$

respectively. To prove Theorem 4, we have only to prove that the above formal power series $F(x)$ is a rational function whose denominator is $\prod_{0\leqq j\leqq n}(1-p^{(n-j)(n+j+1-2s)/2}x)$. Obviously $F(x)=\sum_{0\leqq k\leqq h\leqq n}F(x; k, h)$ holds.

Lemma 12. *For $0\leqq k\leqq h\leqq n$ we have*

$$F(x; k, h)=F(0; k, h)+c(k, h)p^{(k-n)s}x\sum_{h\leqq f\leqq n}F(x; h, f)$$

where

$$c(k, h)=p^{(n-k)(n+k+3)/2+h-n}\prod_{\substack{1\leqq i\leqq h-k\\ i:even}}(1-p^{-i})^{-1}\prod_{k+1\leqq i\leqq h}(p^{-i}-1).$$

Proof. For $\lambda=(0, \cdots, 0, \lambda_{k+1}, \cdots, \lambda_n)\in\Lambda_{k,h}$ we denote $(0, \cdots, 0, \lambda_{h+1}-1, \cdots, \lambda_n-1)\in\Lambda_h$ by $\mu=\lambda-1$. The mapping $\lambda\mapsto\lambda-1$ gives obviously a bijection from $\Lambda_{k,h}$ to Λ_h. Putting $P=\mathrm{diag}(p^{\lambda_{h+1}-1}, \cdots, p^{\lambda_n-1})$, we have

$$\chi(\lambda)=\begin{bmatrix}1_k & & \\ & p1_{h-k} & \\ & & pP\end{bmatrix}, \quad \chi(\mu)=\begin{bmatrix}1_h & \\ & P\end{bmatrix} \quad \text{and } P\equiv 0 \bmod p.$$

It is easy to see that for $U=\begin{bmatrix}U_1^{(k)} & U_2 & U_3\\ U_4 & U_5^{(h-k)} & U_6\\ U_7 & U_8 & U_9\end{bmatrix}\in M_n(Z_p)$, $U\in GL^n(Z_p)\cap$

$\chi(\lambda)^{-1}GL_n(Z_p)\chi(\lambda)$ if and only if $U_1 \in GL_k(Z_p)$, $U_5 \in GL_{h-k}(Z_p)$, $U_9 \in GL_{n-h}(Z_p)$, $U_2 \equiv 0 \bmod p$, $U_3 \in pM_{k,n-h}(Z_p)P$, $U_6 \in M_{h-k,n-h}(Z_p)P$ and $U_9 \in GL_{n-h}(Z_p) \cap P^{-1}GL_{n-h}(Z_p)P$, and for $V=\begin{bmatrix} V_1^{(h)} & V_2 \\ V_3 & V_4 \end{bmatrix} \in M_n(Z_p)$,

$$V \in GL_n(Z_p) \cap \chi(\mu)^{-1}GL_n(Z_p)\chi(\mu)$$

if and only if $V_1 \in GL_h(Z_p)$, $V_4 \in GL_{n-h}(Z_p)$, $V_2 \in M_{h,n-h}(Z_p)P$ and $V_4 \in GL_{n-h}(Z_p) \cap P^{-1}GL_{n-h}(Z_p)P$. Hence $GL_n(Z_p) \cap \chi(\lambda)^{-1}GL_n(Z_p)\chi(\lambda) \subset GL_n(Z_p) \cap \chi(\mu)^{-1}GL_n(Z_p)\chi(\mu)$ holds and then we have

$$\begin{aligned}
&\sum_{U \in G_n(\lambda)} R_n(p^tT[U^{-1}], \mu) \\
&\quad = [GL_n(Z_p) \cap \chi(\mu)^{-1}GL_n(Z_p)\chi(\mu) : GL_n(Z_p) \cap \chi(\lambda)^{-1}GL_n(Z_p)\chi(\lambda)] \\
&\qquad \times \sum_{U \in G_n(\mu)} R_n(p^tT[U^{-1}], \mu)
\end{aligned}$$

since $R_n(T[U], \mu)=R_n(T, \mu)$ for $U \in GL_n(Z_p) \cap \chi(\mu)^{-1}GL_n(Z_p)\chi(\mu)$. The index is equal to $p^{k(n-k)} \prod_{k+1\leqq i\leqq h}(p^{-i}-1) \prod_{1\leqq i\leqq h-k}(p^{-i}-1)^{-1}$ by [1]. Now we have

$$\begin{aligned}
&F(x; k, h) \\
&\quad = F(0; k, h) + \sum_{t\geqq 1}\Big(\sum_{\lambda \in A_{k,h}} w(\lambda)p^{-(\Sigma\lambda_i)s} \sum_{U \in G_n(\lambda)} R_n(p^tT[U^{-1}], \lambda)\Big)x^t \\
&\quad = F(0; k, h) + p^{(n-k)(n-k+1)/2} \prod_{\substack{1\leqq i\leqq h-k \\ i:odd}} (1-p^{-i}) \\
&\qquad \times \sum_{t\geqq 1}\Big(\sum_{\lambda \in A_{k,h}} w(\lambda)p^{-(\Sigma\lambda_i)s} \sum_{U \in G_n(\lambda)} R_n(p^{t-1}T[U^{-1}], \lambda-1)\Big)x^t \\
&\quad = F(0; k, h) + p^{(n-k)(n-k+1)/2} \prod_{\substack{1\leqq i\leqq h-k \\ i:odd}} (1-p^{-i}) \\
&\qquad \times p^{(n-k)k} \prod_{k+1\leqq i\leqq h} (p^{-i}-1) \prod_{1\leqq i\leqq h-k} (p^{-i}-1)^{-1} \\
&\qquad \times x \sum_{t\geqq 0}\Big(\sum_{\lambda \in A_{k,h}} w(\lambda)p^{-(\Sigma\lambda_i)s} \sum_{U \in G_n(\lambda-1)} R_n(p^tT[U^{-1}], \lambda-1)\Big)x^t \\
&\quad = F(0; k, h) + p^{(n-k)(n+k+3)/2-(n-k)s}(-1)^{n-k} \prod_{\substack{1\leqq i\leqq h-k \\ i:odd}} (1-p^{-i}) \\
&\qquad \times \prod_{k+1\leqq i\leqq h} (p^{-i}-1) \prod_{1\leqq i\leqq h-k} (p^{-i}-1)^{-1} \\
&\qquad \times x \sum_{t\geqq 0}\Big(\sum_{\mu \in A_h} p^{-(\Sigma\mu_i)s} \sum_{U \in G_n(\mu)} R_n(p^tT[U^{-1}], \mu)\Big)x^t \\
&\quad = F(0; k, h) + p^{(n-k)(n+k+3)/2+h-n-(n-k)s} \prod_{\substack{1\leqq i\leqq h-k \\ i:even}} (1-p^{-i})^{-1} \\
&\qquad \times \prod_{k+1\leqq i\leqq h} (p^{-i}-1) \cdot x \sum_{h\leqq f\leqq n} F(x; h, f) \\
&\quad = F(0; k, h) + c(k, h)p^{(k-n)s} x \sum_{h\leqq f\leqq n} F(x; h, f).
\end{aligned}$$

Lemma 13. *For* $0 \leqq a \leqq n$ *we have*

$$\prod_{0 \leqq j \leqq a} (1 - p^{(n-j)(n+j+1-2s)/2} x) F(x)$$
$$= \text{a polynomial in } x \text{ of degree } a$$
$$+ x^{a+1} \sum_{a+1 \leqq k \leqq h \leqq n} A(a, k) F(x; k, h),$$

where $A(a, k)$ *is inductively defined as follows*:

$$A(0, k) = \Big(\sum_{0 \leqq g \leqq k} c(g, k) p^{gs} - p^{n(n+1)/2}\Big) p^{-ns} \qquad \text{for } 1 \leqq k \leqq n,$$
$$A(a+1, k) = \sum_{a+1 \leqq g \leqq k} A(a, g) c(g, k) p^{(g-n)s}$$
$$- A(a, k) p^{(n-a-1)(n+a+2-2s)/2} \qquad \text{for } a+2 \leqq k \leqq n.$$

Proof. We use the induction on a. For $a=0$ we have

$$(1 - p^{n(n+1-2s)/2} x) F(x)$$
$$= F(0) + \sum_{0 \leqq k \leqq h \leqq n} c(k, h) p^{(k-n)s} x \sum_{h \leqq f \leqq n} F(x; h, f)$$
$$- p^{n(n+1-2s)/2} x \sum_{0 \leqq k \leqq h \leqq n} F(x; k, h)$$
$$= F(0) + p^{-ns} x \sum_{0 \leqq k \leqq h \leqq n} F(x; k, h) \Big\{ \sum_{0 \leqq g \leqq k} c(g, k) p^{gs} - p^{n(n+1)/2} \Big\}$$
$$= F(0) + x \sum_{1 \leqq k \leqq h \leqq n} A(0, k) F(x; k, h).$$

Suppose that the assertion is true for a; then we have

$$\prod_{0 \leqq j \leqq a+1} (1 - p^{(n-j)(n+j+1-2s)/2} x) F(x)$$
$$= (1 - p^{(n-a-1)(n+a+2-2s)/2} x) \{a \text{ polynomial in } x \text{ of degree } a$$
$$+ x^{a+1} \sum_{a+1 \leqq k \leqq h \leqq n} A(a, k) F(x; k, h)\}$$
$$= \text{a polynomial in } x \text{ of degree } a+1$$
$$+ x^{a+1} \sum_{a+1 \leqq k \leqq h \leqq n} A(a, k) F(x; k, h)$$
$$- p^{(n-a-1)(n+a+2-2s)/2} x^{a+2} \sum_{a+1 \leqq k \leqq h \leqq n} A(a, k) F(x; k, h)$$
$$= \text{a polynomial in } x \text{ of degree } a+1$$
$$+ x^{a+1} \sum_{a+1 \leqq k \leqq h \leqq n} A(a, k) c(k, h) p^{(k-n)s} x \sum_{h \leqq f \leqq n} F(x; h, f)$$
$$- p^{(n-a-1)(n+a+2-2s)/2} x^{a+2} \sum_{a+1 \leqq k \leqq h \leqq n} A(a, k) F(x; k, h)$$

$$=\text{a polynomial in } x \text{ of degree } a+1$$
$$+x^{a+2}\sum_{a+1\leqq k\leqq h\leqq n}F(x;k,h)\{\sum_{a+1\leqq g\leqq k}A(a,g)c(g,k)p^{(g-n)s}$$
$$-p^{(n-a-1)(n+a+2-2s)/2}A(a,k)\}$$
$$=\text{a polynomial in } x \text{ of degree } a+1$$
$$+x^{a+2}\sum_{a+2\leqq k\leqq h\leqq n}F(x;k,h)A(a+1,k),$$

since the coefficient of $F(x;a+1,h)$ vanishes. Thus we have proved Lemma 13 and hence Theorem 4, putting $a=n$.

In order to show that the denominator of $f(x)$ in Theorem 4 is $\prod_{2\leqq j\leqq n}(1-p^{-j(j-1)/2}x)$ in the case of $n=r+2$, it is necessary and sufficient to show $A(n-2,n-1)\sum_{n-1\leqq h\leqq n}F(x;n-1,h)+A(n-2,n)F(x;n,n)=0$ for $s=n$. We show hereafter that the coefficients of the formal power series $F(x;n-1,n-1)$, $F(x;n-1,n)$, $F(x;n,n)$ do not have a pole at $s=n$. Hence $A(n-2,n-1)=A(n-2,n)=0$ at $s=n$ is sufficient for the denominator of $f(x)$ to be $\prod_{2\leqq j\leqq n}(1-p^{-j(j-1)/2}x)$.

Lemma 14. *The coefficients of the formal power series $F(x;n-1,n-1)$, $F(x;n-1,n)$, $F(x;n,n)$ do not have a pole at $s=n$.*

Proof. First we note that $\Lambda_{n,n}=\{(0,\cdots,0)\}$, $\Lambda_{n-1,n}=\{(0,\cdots,0,1)\}$, $\Lambda_{n-1,n-1}=\{(0,\cdots,0,a)\,|\,a\geqq 2\}$. Hence the assertion is obvious from the definition for $F(x;n-1,n)$, $F(x;n,n)$. By definition, $F(x;n-1,n-1)$ is equal to

$$-p\sum_{t\geqq 0}\sum_{a\geqq 2}p^{-as}\sum_{U\in G_n((0,\cdots,0,a))}R_n(p^tT[U^{-1}],(0,\cdots,0,a))x^t.$$

It is not hard to see that the correspondence $U\mapsto$ the transpose of the n-th column of U^{-1} is the bijective mapping from $G_n((0,\cdots,0,a))$ to $\{(x_1,\cdots,x_n)\,|\,x_i\in \boldsymbol{Z}_p,(x_1,\cdots,x_n)=1\}/\underset{a}{\sim}$ where $(x_1,\cdots,x_n)\underset{a}{\sim}(y_1,\cdots,y_n)$ if and only if there is an element $w\in \boldsymbol{Z}_p^\times$ such that $(x_1,\cdots,x_n)\equiv w(y_1,\cdots,y_n)\bmod p^a$. Using the claim at the beginning of the proof of Lemma 11, the coefficient $c(p^tT)$ of x^t of $(-p)^{-1}F(x;n-1,n-1)$ is

$$\sum_{a\geqq 2}p^{-as}\sum_{\{(x_1,\cdots,x_n)|(x_1,\cdots,x_n)=1\}/\underset{a}{\sim}}R_1(p^tT[x],a)$$
$$=\sum_{a\geqq 2}p^{-as}\sum_{\{(x_1,\cdots,x_n)|(x_1,\cdots,x_n)=1\}/\underset{a}{\sim}}\ \sum_{\substack{d \bmod p^a\\(d,p)=1}}e(p^tT[x]d/p^a).$$

We have only to prove that this is, in fact a polynomial in p^{-s}. It is easy to see

$$\sum_{\substack{x_i \bmod p^a \\ (x_1,\cdots,x_n)=1}} \sum_{\substack{d \bmod p^a \\ (d,p)=1}} e(p^t T[x]d/p^a)$$

$$= \sum_{\{(x_1,\cdots,x_n)\mid(x_1,\cdots,x_n)=1\}/\sim} \sum_{\substack{y \bmod p^a \\ (y,p)=1}} \sum_{\substack{d \bmod p^a \\ (d,p)=1}} e(p^t T[x]y^2 d/p^a)$$

$$= p^a(1-p^{-1}) \sum_{\{(x_1,\cdots,x_n)\mid(x_1,\cdots,x_n)=1\}/\sim} \sum_{\substack{d \bmod p^a \\ (d,p)=1}} e(p^t T[x]d/p^a).$$

Therefore, putting $D(p^tT, a)=\sum_{x_i \bmod p^a} \sum_{\substack{d \bmod p^a \\ (d,p)=1}} e(p^tT[x]d/p^a)$, we have

$$\sum_{\{(x_1,\cdots,x_n)\mid(x_1,\cdots,x_n)=1\}/\sim} \sum_{\substack{d \bmod p^a \\ (d,p)=1}} e(p^t T[x]d/p^a)$$

$$= p^{-a}(1-p^{-1})^{-1}\{D(p^tT, a) - p^{n+2}D(p^tT, a-2)\}.$$

To evaluate $D(p^tT, a)$, we may suppose $T=\mathrm{diag}\,(\varepsilon_1 p^{b_1}, \cdots, \varepsilon_n p^{b_n})$, $\varepsilon_i \in Z_p^\times$, $0 \leqq b_1 \leqq \cdots \leqq b_n$. If $a > b_n + t$, then

$$D(p^tT, a) = \sum_{\substack{x_i \bmod p^a \\ d \bmod p^a \\ (d,p)=1}} e(d \sum_{i=1}^{n} \varepsilon_i p^{b_i} x_i^2 / p^{a-t})$$

$$= \sum_{\substack{d \bmod p^a \\ (d,p)=1}} \prod_{i=1}^{n} \sum_{x \bmod p^a} e(\varepsilon_i d x^2 / p^{a-t-b_i})$$

$$= \sum_{\substack{(d,p)=1 \\ d \bmod p^a}} \prod_{i=1}^{n} p^{t+b_i} \sum_{x \bmod p^{a-t-b_i}} e(\varepsilon_i d x^2 / p^{a-t-b_i})$$

$$= p^{nt+\Sigma b_i} \sum_{\substack{d \bmod p^a \\ (d,p)=1}} \prod_{i=1}^{n} p^{(a-t-b_i)/2} \left(\frac{\varepsilon_i d}{p}\right)^{a-t-b_i} \times \begin{cases} 1 & p^{a-t-b_i} \equiv 1 \bmod 4, \\ \sqrt{-1} & p^{a-t-b_i} \equiv 3 \bmod 4 \end{cases}$$

$$= p^{(nt+\Sigma b_i)/2 + na/2 + a - 1} \sum_{\substack{d \bmod p \\ (d,p)=1}} \prod_{i=1}^{n} \left(\frac{\varepsilon_i d}{p}\right)^{a-t-b_i} \times \begin{cases} 1 & p^{a-t-b_i} \equiv 1 \bmod 4, \\ \sqrt{-1} & p^{a-t-b_i} \equiv 3 \bmod 4. \end{cases}$$

Hence $D(p^tT, a+2) = p^{n+2}D(p^tT, a)$ follows for $a > b_n + t$ and the coefficient of x^t of $F(x; n-1, n-1)$ is a polynomial in p^{-s}. Thus Lemma 14 has been proved.

The condition $A(n-2, n-1) = A(n-2, n) = 0$ at $s=n$ is easily transformed to the one stated in the introduction.

References

[1] A. N. Andrianov, Spherical functions for GL_n over local fields, and summation of Hecke series, Math. USSR Sbornik, **12** (1970), 429–452.
[2] ——, Integral representations of quadratic forms by quadratic forms: Multiplicative Properties, Proc. of the International Congress of Math. 1983, Warszawa, 465–474.
[3] J. S. Hsia, Regular positive ternary quadratic forms, Mathematika, **28** (1981), 231–238.
[4] J. S. Hsia, Y. Kitaoka and M. Kneser, Representations of positive definite quadratic forms, J. Reine Angew. Math., **301** (1978), 132–141.
[5] Y. Kitaoka, A note on local densities of quadratic forms, Nagoya Math. J., **92** (1983), 145–152.
[6] ——, Lectures on Siegel modular forms and representation by quadratic forms, Tata Institute of Fundamental Research, 1986.
[7] ——, Local densities of quadratic forms and Fourier coefficients of Eisenstein series, Nagoya Math. J., **103** (1986), 149–160.
[8] ——, Modular forms of degree n and representation by quadratic forms IV, Nagoya Math. J., **107** (1987), to appear.
[9] M. Kneser, Quadratische Formen, Vorlesungs-Ausarbeitung, Göttingen, 1973–74.
[10] O. T. O'Meara, Introduction to quadratic forms, Springer-Verlag, 1973.
[11] F. Sato, The rationality of a certain formal power series related to local densities of quratic forms, to appear.
[12] C. L. Siegel, Über die analytische Theorie der quadratischen Formen, Ann. of Math., **36** (1935), 527–607.
[13] H. Yoshida, On Siegel modular forms obtained from theta series, J. Reine Angew. Math., **352** (1984), 184–219.

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