Bull. Korean Math. Soc. **61** (2024), No. 4, pp. 907–915
https://doi.org/10.4134/BKMS.b230293
pISSN: 1015-8634 / eISSN: 2234-3016

A NOTE ON REPRESENTATION NUMBERS OF QUADRATIC FORMS MODULO PRIME POWERS

Ran Xiong

Abstract. Let f be an integral quadratic form in k variables, F the Gram matrix corresponding to a $\mathbb{Z}$-basis of $\mathbb{Z}^k$. For $r \in F^{-1}\mathbb{Z}^k$, a rational number n with $f(r) \equiv n \bmod \mathbb{Z}$ and a positive integer c, set $N_f(n, r; c) := \sharp\{x \in \mathbb{Z}^k/c\mathbb{Z}^k : f(x + r) \equiv n \bmod c\}$. Siegel showed that for each prime p, there is a number w depending on r and n such that $N_f(n, r; p^{\nu+1}) = p^{k-1}N_f(n, r; p^\nu)$ holds for every integer $\nu > w$ and gave a rough estimation on the upper bound for such w. In this short note, we give a more explicit estimation on this bound than Siegel's.

1. Introduction and statement

Let f be an integral quadratic form in k variables, F the Gram matrix corresponding to a $\mathbb{Z}$-basis of $\mathbb{Z}^k$. For $r \in F^{-1}\mathbb{Z}^k$, a rational number n with $f(r) \equiv n \bmod \mathbb{Z}$ and a positive integer c, set

$$N_f(n, r; c) := \sharp\{x \in \mathbb{Z}^k/c\mathbb{Z}^k : f(x + r) \equiv n \bmod c\}. \tag{1.1}$$

In his seminal work for representation numbers of quadratic forms, Siegel [5] in fact proved that for a nonzero n,

$$N_f(n, r; p^{\nu+1}) = p^{k-1}N_f(n, r; p^\nu) \quad \text{when } \nu > \nu_p(2\omega_r^2 n^2) \tag{1.2}$$

(see [5, Hilfssatz 13]. For a clearer form one can also refer to [3, Lemma 5]). Here ω_r is the smallest positive integer such that $\omega_r r \in \mathbb{Z}^k$. In this paper, by computing $N_f(n, r; p^{\nu+1})$ with the method of Gauss sums we improve the Siegel's result. Roughly saying we find that

$$N_f(n, r; p^{\nu+1}) = p^{k-1}N_f(n, r; p^\nu) \quad \text{when} \quad \nu > \nu_p(2\omega_r^2 n).$$

We explain the above statement more explicitly by the language of lattice. Recall that an even *lattice* $\underline{L} = (L, \beta)$ is a free $\mathbb{Z}$-module L of finite rank $\mathrm{rk}(\underline{L})$, equipped with a non-degenerate symmetric $\mathbb{Z}$-valued bilinear form β such that $\beta(x) := \beta(x, x)/2 \in \mathbb{Z}$ for all $x \in L$. Note that $\beta : L \to \mathbb{Z}$ is a quadratic form, i.e., $\beta(ax) = a^2\beta(x)$ for all $a \in \mathbb{Z}$ and $x \in L$. In the following by writing an even

Received May 14, 2023; Revised February 22, 2024; Accepted February 29, 2024.
2020 *Mathematics Subject Classification.* 11D9, 11D85.
Key words and phrases. Representation numbers of quadratic forms, Gauss sums, lattices.

lattice (L, β), β refers to the quadratic form which is induced by the symmetric $\mathbb{Z}$-valued bilinear form. For example, $(\mathbb{Z}, x^2)$ is the lattice $(\mathbb{Z}, (x,y) \to 2xy)$.

The dual of lattice $\underline{L}$ is

$$L^\sharp = \{y \in L \otimes_{\mathbb{Z}} \mathbb{Q} : \beta(x,y) \in \mathbb{Z} \quad \text{for all } x \in L\}.$$

It is well known that $|L^\sharp/L|$ equals to $|\det(\underline{L})|$, where $\det(\underline{L})$ is the determinant of the Gram matrix corresponding to any $\mathbb{Z}$-basis of L thus $L^\sharp/L$ is a finite abelian group. Define $\Delta(\underline{L})$, $\ell(\underline{L})$, the discriminant of $\underline{L}$ and the level of $\underline{L}$ as follows:

$$\Delta(\underline{L}) := \begin{cases} (-1)^{\lfloor \frac{\mathrm{rk}(\underline{L})}{2} \rfloor} \det(\underline{L}) & \text{if } \mathrm{rk}(\underline{L}) \text{ is even;} \\ (-1)^{\lfloor \frac{\mathrm{rk}(\underline{L})}{2} \rfloor} 2\det(\underline{L}) & \text{if } \mathrm{rk}(\underline{L}) \text{ is odd,} \end{cases}$$

$$\ell(\underline{L}) := \min\{\ell \in \mathbb{N} : \ell\beta(r) \in \mathbb{Z} \quad \text{for all } r \in L^\sharp\}.$$

For an element $r \in L^\sharp$, let $\omega_{\underline{L}}(r)$ be the order of r in $L^\sharp/L$. Obviously $\ell(\underline{L})|\Delta(\underline{L})$. For any element $x \in L^\sharp$, we have that

$$\beta(\ell(\underline{L})r, x) = \ell(\underline{L})\beta(r,x) = \ell(\underline{L})\left(\beta(r) + \beta(y) - \beta(r+y)\right) \in \mathbb{Z},$$

which implies that $\ell(\underline{L})r \in L$ thus $\omega_{\underline{L}}(r)|\ell(\underline{L})$.

Under the same notations as the above, we rewrite (1.1) as

$$N_{\underline{L}}(n,r;c) := \sharp\{x \in L/cL : \beta(x+r) \equiv n \bmod c\}. \tag{1.3}$$

We put

$$g_{\underline{L}}(n,r;c) := \sum_{d|c} \mu(d) d^{\mathrm{rk}(\underline{L})-1} N_{\underline{L}}(n,r;c/d).$$

Then the Siegel's result is reformulated as

$$g_{\underline{L}}(n,r;p^\nu) = 0 \quad \text{when} \quad \nu > \nu_p(2p\omega_{\underline{L}}(r)^2 n^2). \tag{1.4}$$

Strictly speaking we will prove the following theorem:

Theorem 1.1. *Let $\underline{L} = (L, \beta)$ be an even lattice, r an element in the dual of $\underline{L}$ and n a rational number with $\beta(r) \equiv n \bmod \mathbb{Z}$.*

(1) *For a prime $p \mid \omega_{\underline{L}}(r)$, we have $g_{\underline{L}}(n,r;p^\nu) = 0$ when $\nu > \nu_p(2\ell(\underline{L}))$.*
(2) *Let p be a prime with $p \nmid \omega_{\underline{L}}(r)$.*
 (2i) *If $n \neq 0$ then $g_{\underline{L}}(n,r;p^\nu) = 0$ when $\nu > \nu_p(8p\omega_{\underline{L}}(r)^2 n)$.*
 (2ii) *We have*

$$g_{\underline{L}}(0,r;p^{\nu+2}) = p^{\mathrm{rk}(\underline{L})} g_{\underline{L}}(0,r;p^\nu) \quad \text{when } \nu > \nu_p(2\ell(\underline{L})).$$

We now fix basic notations throughout this paper. For a prime p, $\mathbb{Z}_p$ stands for the ring of p-adic integers. For a rational number a, $\nu_p(a)$ is the p-adic valuation of the rational number a. The bracket $\left(\frac{\cdot}{\cdot}\right)$ is the Kronecker symbol, i.e., for an odd prime p, $\left(\frac{\cdot}{p}\right)$ is the usual Legendre symbol, for $p=2$,

$$\left(\frac{a}{2}\right) := \begin{cases} 0 & \text{if } a \equiv 0 \bmod 2; \\ 1 & \text{if } a \equiv \pm 1 \bmod 8; \\ -1 & \text{if } a \equiv \pm 3 \bmod 8. \end{cases}$$

For an integer c and a complex number t, we write $e_c(t) := e^{\frac{2\pi i t}{c}}$.

2. Proof of Theorem 1.1

Since $g_{\underline{L}}$ is multiplicative in the variable c, we just need to study $g_{\underline{L}}(n,r;p^\nu)$ for prime powers p^ν. For studying we express $g_{\underline{L}}(n,r;p^\nu)$ in terms of Gauss sums as follows:

$$g_{\underline{L}}(n,r;p^\nu) = \frac{1}{p^\nu} \sum_{\substack{d \bmod p^\nu \\ \gcd(d,p)=1}} \sum_{x \in L/p^\nu L} e_{p^\nu}\left(d(\beta(x+r)-n)\right). \tag{2.1}$$

Firstly we have

Lemma 2.1. *Under the same notations as before, we have the following*:

(1) *If $p \mid \omega_{\underline{L}}(r)$, then*

$$g_{\underline{L}}(n,r;p^\nu) = \frac{1}{p^\nu} \sum_{\substack{d \bmod p^\nu \\ \gcd(d,p)=1}} e_{p^\nu}(dn_r) \sum_{x \in L/p^\nu L} e_{p^\nu}\left(d(\beta(x)+\beta(r,x))\right), \tag{2.2}$$

where $n_r = \beta(r) - n$.

(2) *If $p \nmid \omega_{\underline{L}}(r)$, then*

$$g_{\underline{L}}(n,r;p^\nu) = \frac{1}{p^\nu} \sum_{\substack{d \bmod p^\nu \\ \gcd(d,p)=1}} e_{p^\nu}(-d\omega_{\underline{L}}(r)^2 n) \sum_{x \in L/p^\nu L} e_{p^\nu}(d\beta(x)). \tag{2.3}$$

Proof. The assertion (1) is obvious. For (2), since $p \nmid \omega_{\underline{L}}(r)$, one has

$$\begin{aligned} N_{\underline{L}}(n,r;p^\nu) &= \sharp\{x \in L/p^\nu L : \beta(x+r) \equiv n \bmod p^\nu\} \\ &= \sharp\{x \in L/p^\nu L : \omega_{\underline{L}}(r)^2\beta(x+r) \equiv \omega_{\underline{L}}(r)^2 n \bmod p^\nu\} \\ &= \sharp\{x \in L/p^\nu L : \beta(\omega_{\underline{L}}(r)x + \omega_{\underline{L}}(r)r)) \equiv \omega_{\underline{L}}(r)^2 n \bmod p^\nu\} \\ &= \sharp\{x \in L/p^\nu L : \beta(x) \equiv \omega_{\underline{L}}(r)^2 n \bmod p^\nu\} \\ &= N_{\underline{L}}(\omega_{\underline{L}}(r)^2 n, 0; p^\nu), \end{aligned}$$

where for the fourth identity, we replace $\omega_{\underline{L}}(r)x + \omega_{\underline{L}}(r)r$ by x. Now one can immediately see (2) is true. □

For proving the main theorem, we need some auxiliary lemmas. The following lemma is a key to prove (1) of Theorem 1.1.

Lemma 2.2. *Let $\underline{L} = (L, \beta)$ be an even lattice, r an element in the dual of $\underline{L}$ and p a prime with $p \mid \omega_{\underline{L}}(r)$. Then for each integer $\nu > \nu_p(2\ell(\underline{L}))$, there exists an element y of L such that $p^\nu | \beta(y)$, $p^\nu | \beta(x, y)$ for all $x \in L$, and $p^\nu \nmid \beta(r, y)$.*

Proof. For the sake of simplicity we write ℓ for $\ell(\underline{L})$ and $\ell_p := p^{\nu_p(\ell)}$. By the definition of level, we know that the denominator of $(\ell/\ell_p)\beta(r)$ is a p-power (including one). The assumption $p|\omega_{\underline{L}}(r)$ implies that the order of the element $(\ell/\ell_p)r$ is a p-power more than one thus for each $y \in L$, the possible denominator of $\beta((\ell/\ell_p)r, y)$ is also a power of the prime p.

If $(\ell/\ell_p)\beta(r) \notin \mathbb{Z}$, then we let $y = 2p^\nu(\ell/\ell_p)r$. Obviously $p^\nu|\beta(x, y)$ for all $x \in L$. Since $\nu > \nu_p(2\ell_p)$, $p^\nu/\ell_p \in \mathbb{Z}$ thus $y = (p^\nu/\ell_p)\ell r \in L$. We have

$$\beta(y) = \frac{\beta(p^\nu(\ell/\ell_p)r, p^\nu(\ell/\ell_p)r)}{2} = p^\nu \cdot (p^\nu/\ell_p) \cdot (\ell/\ell_p)\ell\beta(r) \in p^\nu\mathbb{Z}.$$

Also $(\ell/\ell_p)\beta(r) \notin \mathbb{Z}$ means that the p-valuation of $(\ell/\ell_p)\beta(r)$ is negative thus $\beta(r, y) = p^\nu(\ell/\ell_p)\beta(r) \notin p^\nu\mathbb{Z}$. By the above discussion, the element $y \in L$ exists as the lemma claimed.

If $(\ell/\ell_p)\beta(r) \in \mathbb{Z}$, then the pair $(L\langle(\ell/\ell_p)r\rangle, \beta)$ is also an even lattice. Here $L\langle(\ell/\ell_p)r\rangle$ is the $\mathbb{Z}$-module, which is generated by L and $(\ell/\ell_p)r$. Note that the element $(\ell/\ell_p)r$ is not in L. We have

$$|L^\sharp : L\langle(\ell/\ell_p)r\rangle^\sharp| = |L\langle(\ell/\ell_p)r\rangle : L| > 1,$$

which implies that there exists an element y' in $L^\sharp$ such that $\beta((\ell/\ell_p)r, y') \notin \mathbb{Z}$ thus the p-adic valuation is negative. Now one can check that $y = p^\nu y'$ as the lemma stated. ∎

For proving (2i) of Theorem 1.1 we need:

Lemma 2.3. *Let $\underline{L} = (L, \beta)$ be an even lattice. For each prime power p^ν, the following*

$$\sum_{x \in L/p^\nu L} e_{p^\nu}\left((d + 4p)\beta(x)\right) = \sum_{x \in L/p^\nu L} e_{p^\nu}\left(d\beta(x)\right)$$

holds for any integer d coprime to p.

Proof. For each integer d coprime to p, one can find an integer t coprime to p satisfying $dt^2 \equiv d + 4p \bmod p^\nu$. The application $x \to tx$ is an automorphism of $L/p^\nu L$ thus

$$\sum_{x \in L/p^\nu L} e_{p^\nu}\left(d\beta(x)\right) = \sum_{x \in L/p^\nu L} e_{p^\nu}\left(d\beta(tx)\right)$$
$$= \sum_{x \in L/p^\nu L} e_{p^\nu}\left(dt^2\beta(x)\right) = \sum_{x \in L/p^\nu L} e_{p^\nu}\left((d + 4p)\beta(x)\right).$$

This proves the lemma. ∎

To prove (2ii) of Theorem 1.1 we shall evaluate $\sum_{x\in L/p^\nu L} e_{p^\nu}(d\beta(x))$ for $\nu > \nu_p(2\ell(\underline{L}))$. We briefly introduce the terminology of Jordan decomposition over the ring of p-adic integers. Define the following lattices over the ring of p-adic integers:

(i) $\underline{A}^{\varepsilon}_{p^j} := \left(\mathbb{Z}_p, p^j\varepsilon x^2\right)$, p is odd prime, $\gcd(p,\varepsilon)=1$;
(ii) $\underline{A}^{\varepsilon}_{2^j} := \left(\mathbb{Z}_2, 2^{j+1}\varepsilon x^2\right)$, $\gcd(2,\varepsilon)=1$;
(iii) $\underline{B}_{2^j} := \left(\mathbb{Z}_2\times\mathbb{Z}_2, 2^j\left(x^2+xy+y^2\right)\right)$;
(iv) $\underline{C}_{2^j} := \left(\mathbb{Z}_2\times\mathbb{Z}_2, 2^j xy\right)$.

For an even lattice $\underline{L}=(L,\beta)$ set $\underline{L}_p := (L\otimes\mathbb{Z}_p,\beta)$ and we simply write $L\otimes\mathbb{Z}_p$ as L_p. We say that two $\mathbb{Z}_p$-lattices (L_p,β) and (L'_p,β') are isomorphic over $\mathbb{Z}_p$ if there is an isomorphism ψ from L_p to L'_p such that for each $x\in L$, $\beta(x)=\beta(\psi(x))$ holds. The *Jordan decomposition* over the ring of p-adic integers shows that lattices over $\mathbb{Z}_p$ can be isomorphic to direct sums of the above $\mathbb{Z}_p$-lattices, which is the following proposition:

Proposition 2.4 ([4, Chapter 15, Theorem 2]). *Let $\underline{L}=(L,\beta)$ be an even lattice.*

(1) *For any odd prime p, $\underline{L}_p$ is isomorphic to the form*

$$\underline{L}_p \approx \bigoplus_{j=0}^{l_p}\bigoplus_{i=0}^{r_{p,j}} \underline{A}^{\varepsilon_{p^j,i}}_{p^j}; \tag{2.4}$$

(2) *The lattice $\underline{L}$ is isomorphic to the following form over $\mathbb{Z}_2$:*

$$\underline{L}_2 \approx \Big(\bigoplus_{j=1}^{l_2}\bigoplus_{i=0}^{r_{2,j}} \underline{A}^{\varepsilon_{2^j,i}}_{2^j}\Big) \oplus \Big(\bigoplus_{j=1}^{m_2}\big(\underbrace{\underline{B}_{2^j}\oplus\cdots\oplus\underline{B}_{2^j}}_{s_j}\oplus\underbrace{\underline{C}_{2^j}\oplus\cdots\oplus\underline{C}_{2^j}}_{t_j}\big)\Big). \tag{2.5}$$

Remark 2.5. We admit that $r_{p,j}$, $r_{2,j}$, s_j, t_j are zero. If we let l_p(resp. l_2, m_2) be the smallest integer such that $r_{p,j}$(resp. $r_{2,j}$, s_j+t_j) $=0$ when $j>l_p$(resp. l_2, m_2), then $\nu_p(\ell(\underline{L}))=l_p$ for any odd prime and $\nu_2(\ell(\underline{L}))=\max\{l_2+2, m_2\}$.

We also need some results for classical Gauss sums.

Lemma 2.6 ([2, Chapter 1]). *Let p be an odd prime and d an integer with $p\nmid d$. For a positive integer ν we have*

$$\sum_{x \bmod p^\nu} e_{p^\nu}(dx^2) = \epsilon(p^\nu)p^{\frac{\nu}{2}}\left(\frac{d}{p^\nu}\right),$$

where for an odd integer m, $\epsilon(m) := \sqrt{\left(\frac{-1}{m}\right)}$.

Lemma 2.7 ([2, Chapter 1]). *For each positive integer ν and odd integer d, one has*

$$\sum_{x \bmod 2^\nu} e_{2^\nu}(dx^2) = \begin{cases} 0 & \text{if } \nu = 1; \\ 2^{\frac{\nu+1}{2}} \left(\dfrac{d}{2^{\nu+1}}\right) e_8(d) & \text{if } \nu > 1. \end{cases}$$

Lemma 2.8 ([1, Lemma 2.1.9, 2.1.10]). *For each positive integer ν and odd integer d, the following identities hold*:

$$\sum_{x,y \bmod 2^\nu} e_{2^\nu}(dxy) = 2^\nu \left(\frac{-1}{2^\nu}\right), \qquad \sum_{x,y \bmod 2^\nu} e_{2^\nu}(d(x^2+xy+y^2)) = 2^\nu \left(\frac{3}{2^\nu}\right).$$

Lemma 2.9. *Let $\underline{L} = (L, \beta)$ be an even lattice. Write*

$$\gamma_{\underline{L}}(d,c) := \sum_{x \in L/cL} e_c(d\beta(x))$$

for positive integer c and integer d. For any prime p and d coprime to p, the identity $\gamma_{\underline{L}}(d, p^{\nu+2}) = p^{\mathrm{rk}(\underline{L})} \gamma_{\underline{L}}(d, p^\nu)$ holds when $\nu > \nu_p(2\ell(\underline{L}))$.

Proof. Let $\underline{L} = (L, \beta)$ be an even lattice whose Jordan decomposition over $\mathbb{Z}_p$ as stated in Proposition 2.4 for each prime p. For an odd prime power $p^\nu > p^{\nu_p(2\ell_{\underline{L}})}$ and an integer d coprime to p, applying Lemma 2.6 we have

$$\begin{aligned} \gamma_{\underline{L}}(d, p^\nu) &= \sum_{x \in L/p^\nu L} e_{p^\nu}(d\beta(x)) \\ &= \prod_{j=0}^{\nu_p(\ell(\underline{L}))} \prod_{i=0}^{r_{p,j}} \left(\sum_{x \bmod p^\nu} e_{p^\nu}(dp^j \varepsilon_{p^j,i} x^2) \right) \\ &= \prod_{j=0}^{\nu_p(\ell(\underline{L}))} \prod_{i=0}^{r_{p,j}} \left(p^j \sum_{x \bmod p^\nu} e_{p^{\nu-j}}(d\varepsilon_{p^j,i} x^2) \right) \\ &= \prod_{j=0}^{\nu_p(\ell(\underline{L}))} p^{\frac{r_{p,j}(\nu+j)}{2}} \epsilon(p^{\nu-j})^{r_{p,j}} \prod_{i=0}^{r_{p,j}} \left(\frac{\varepsilon_{p^j,i} d}{p^{\nu+j}} \right). \end{aligned} \tag{2.6}$$

For $\nu > \nu_2(2\ell_{\underline{L}})$ and an odd integer d, one has

$$\begin{aligned} \gamma_{\underline{L}}(d, 2^\nu) &= \sum_{x \in L/2^\nu L} e_{2^\nu}(d\beta(x)) \\ &= \prod_{j=0}^{b_2} \left(\sum_{x,y \bmod 2^\nu} e_{2^\nu}(d2^j(x^2+xy+y^2)) \right)^{s_j} \\ &\quad \times \prod_{j=0}^{c_2} \left(\sum_{x,y \bmod 2^\nu} e_{2^\nu}(d2^j xy) \right)^{t_j} \prod_{j=0}^{a_2} \prod_{i=1}^{r_{2,j}} \left(\sum_{x \bmod 2^\nu} e_{2^\nu}(d2^j \varepsilon_{2^j,i} x^2) \right). \end{aligned}$$

By applying Lemmas 2.7 and 2.8, we get

$$
\begin{aligned}
(2.7)\quad & \gamma_{\underline{L}}(d, 2^\nu) \\
&= \prod_{j=0}^{b_2} \left(2^{\nu+j} \left(\frac{3}{2^{\nu+j}} \right) \right)^{s_j} \prod_{j=0}^{c_2} \left(2^{\nu+j} \left(\frac{-1}{2^{\nu+j}} \right) \right)^{t_j} \\
&\quad \times \prod_{j=0}^{a_2} \left(2^{\frac{\nu+j+1}{2}} \left(\frac{d}{2^{\nu+j+1}} \right) \right)^{r_{2,j}} \prod_{j=0}^{a_2} \prod_{i=0}^{r_{2,j}} \left(\frac{\varepsilon_{2^j,i}}{2^{\nu+j+1}} \right) e_8 \left(\sum_{j=0}^{a_2} \sum_{i=0}^{r_{2,j}} \varepsilon_{2^j,i} d \right) \\
&= 2^{\frac{\nu \sum (s_j+t_j+r_{2,j})}{2}} \prod_{j=0}^{b_2} \left(2^{j} \left(\frac{3}{2^{j}} \right) \right)^{s_j} \prod_{j=0}^{c_2} \left(2^{\nu+j} \left(\frac{-1}{2^{j}} \right) \right)^{t_j} \\
&\quad \times \prod_{j=0}^{a_2} \left(2^{\frac{j+1}{2}} \left(\frac{d}{2^{j+1}} \right) \right)^{r_{2,j}} \prod_{j=0}^{a_2} \prod_{i=0}^{r_{2,j}} \left(\frac{\varepsilon_{2^j,i}}{2^{j+1}} \right).
\end{aligned}
$$

Now by the relation

$$\sum_j r_{p,j} = \sum_j (s_j + t_j + r_{2,j}) = \mathrm{rk}(\underline{L}),$$

one immediately sees the lemma is true after observing last identities of (2.6) and (2.7). □

Proof of Theorem 1.1. (1) We use the expression for $g_{\underline{L}}(n, r; p^\nu)$ as in (2.2). It is sufficient to show that for any prime $p | \omega_{\underline{L}}(r)$ and integer ν more than $\nu_p(2\ell(\underline{L}))$, the inner sum of (2.2) vanishes. Recall that the inner sum of (2.2) is

$$(2.8)\qquad \sum_{x \in L/p^\nu L} e_{p^\nu} \left(d \left(\beta(x) + \beta(r, x) \right) \right).$$

From Lemma 2.2 we know that for each integer $\nu > \nu_p(2\ell(\underline{L}))$, there exists an element y of L such that $p^\nu | \beta(y)$, $p^\nu | \beta(x, y)$ for all $x \in L$, and $p^\nu \nmid \beta(r, y)$. Replacing x by $x + y$ we have

$$
\begin{aligned}
& \sum_{x \in L/p^\nu L} e_{p^\nu} \left(d \left(\beta(x) + \beta(r, x) \right) \right) \\
&= \sum_{x \in L/p^\nu L} e_{p^\nu} \left(d \left(\beta(x+y) + \beta(r, x+y) \right) \right) \\
&= e_{p^\nu}(\beta(r, y)) \sum_{x \in L/p^\nu L} e_{p^\nu} \left(d \left(\beta(x) + \beta(r, x) \right) \right),
\end{aligned}
$$

which yields that (2.8) equals zero. This proves (1).

(2) We use the expression for $g_{\underline{L},n,r}(p^\nu)$ in (2.3). For (2i), substituting d by $d + 4p$ in (2.3) we have

$$
\begin{aligned}
& p^\nu g_{\underline{L}}(n,r;p^\nu)\\
&= \sum_{\substack{d \bmod p^\nu\\ \gcd(d,p^\nu)=1}} e_{p^\nu}\left(-(d+4p)\omega_{\underline{L}}(r)^2 n\right) \sum_{x\in L/p^\nu L} e_{p^\nu}((d+4p)\beta(x))\\
&= e_{p^\nu}\left(-4p\omega_{\underline{L}}(r)^2 n\right) \sum_{\substack{d \bmod p^\nu\\ \gcd(d,p^\nu)=1}} e_{p^\nu}(-d\omega_{\underline{L}}(r)^2 n) \sum_{x\in L/p^\nu L} e_{p^\nu}\left((d+4p)\beta(x)\right)\\
&= e_{p^{\nu-1}}\left(-4\omega_{\underline{L}}(r)^2 n\right) \sum_{\substack{d \bmod p^\nu\\ \gcd(d,p^\nu)=1}} e_{p^\nu}(-d\omega_{\underline{L}}(r)^2 n) \sum_{x\in L/p^\nu L} e_{p^\nu}\left(d\beta(x)\right)\\
&= e_{p^{\nu-1}}\left(-4\omega_{\underline{L}}(r)^2 n\right) p^\nu g_{\underline{L}}(n,r;p^\nu),
\end{aligned}
$$

where for the third identity we used Lemma 2.3. The number $e_{p^{\nu-1}}\left(-4\omega_{\underline{L}}(r)^2 n\right)$ fails to be an integer when $\nu > \nu_p(8p\omega_{\underline{L}}(r)^2 n)$, which yields that $g_{\underline{L}}(n,r;p^\nu) = 0$. This proves (2i).

Finally we consider (2ii). We have that

$$
g_{\underline{L}}(0,0;p^\nu) = \frac{1}{p^\nu} \sum_{\substack{d \bmod p^\nu\\ \gcd(d,p)=1}} \sum_{x\in L/p^\nu L} e_{p^\nu}(d\beta(x)).
$$

Write $\gamma_{\underline{L}}(d,p^\nu) = \sum_{x\in L/p^\nu L} e_{p^\nu}(d\beta(x))$. By Lemma 2.3, $\gamma_{\underline{L}}(d,p^\nu) = \gamma_{\underline{L}}(d+4p,p^\nu)$ for each integer d with $\gcd(d,p)=1$. Therefore, for each integer $\nu > \nu_p(2\ell(\underline{L}))$, we have

$$
g_{\underline{L}}(0,0;p^{\nu+2}) = \frac{1}{p^{\nu+2}} \sum_{\substack{d \bmod p^{\nu+2}\\ \gcd(d,p)=1}} \gamma_{\underline{L}}(d,p^{\nu+2}) = \frac{1}{p^\nu} \sum_{\substack{d \bmod p^{\nu}\\ \gcd(d,p)=1}} \gamma_{\underline{L}}(d,p^{\nu+2}).
$$

According to Lemma 2.9, $\gamma_{\underline{L}}(d,p^{\nu+2}) = p^{\mathrm{rk}(\underline{L})}\gamma_{\underline{L}}(d,p^\nu)$ holds when $\nu > \nu_p(2\ell(\underline{L}))$. Finally we find that

$$
g_{\underline{L}}(0,0;p^{\nu+2}) = p^{\mathrm{rk}(\underline{L})} \times \frac{1}{p^\nu} \sum_{\substack{d \bmod p^{\nu}\\ \gcd(d,p)=1}} \gamma_{\underline{L}}(d,p^\nu) = p^{\mathrm{rk}(\underline{L})} g_{\underline{L}}(0,0;p^\nu).
$$

Now we complete the proof of Theorem 1.1. □

Acknowledgements. The author would like to thank the referees for their valuable comments on this work. Also the author is greatly indebted to Nils-Peter Skoruppa, for teaching to the author basic knowledge of lattices, finite quadratic modules and related topics during 2015-2019.

References

[1] A. Ajouz, *Hecke operators on Jacobi forms of lattice index and the relation to elliptic modular forms*, Ph.D. thesis, University of Siegen, 2015.

[2] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi Sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, John Wiley & Sons, Inc., New York, 1998.

[3] J. H. Bruinier and M. Kuss, *Eisenstein series attached to lattices and modular forms on orthogonal groups*, Manuscripta Math. **106** (2001), no. 4, 443–459. https://doi.org/10.1007/s229-001-8027-1

[4] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, third edition, Grundlehren Math. Wiss. 290, Springer, New York, 1999. https://doi.org/10.1007/978-1-4757-6568-7

[5] C. L. Siegel, *Über die analytische Theorie der quadratischen Formen*, Ann. of Math. (2) **36** (1935), no. 3, 527–606. https://doi.org/10.2307/1968644

Ran Xiong
School of Mathematics and Statistics
Weinan Normal University
Weinan, 714099, Shanxi, P. R. China
Email address: ranxiong2012@163.com