立命館大学理工学研究所紀要第57号　1998年
Memoirs of Institute of Science and Engineering,Ritsumeikan University,Shiga,Japan.No.57 1998

On the Signature for Finite Quadratic Forms

Isao Naruki and Naoshi Tsuchida

abstract

We give a proof to an explicit formula for the signature of finite quadratic forms which is stated in [2] without proof. We will use Wall's method [4] of constructing even lattice having a given finite quadratic form as its discriminant form, and calculate the signature of the lattice using the product formula of Hilbert symbol and the reciprocity law of the Jacobi symbol.

The Ritsumeikan University, the Faculty of Science and Engineering.

1 Basic notions and preliminaries

This section is divided into two parts, in the first of which we explain some concepts such as the discriminant bilinear forms or quadratic forms etc. concerning lattices over $\boldsymbol{Z}$ or its completions by valuations. In the second part we mention some number theoretic facts which form the main tool of proving the signature formula.

1.1 Lattices and discriminant forms

We let R be the ring $\boldsymbol{Z}$ of rational integers or the ring $\boldsymbol{Z}_p$ of p-adic integers, and Q denotes the quotient field of R.

An *R-lattice* means a finte R-module of finite rank, with a nondegenerate symmetric R-valued bilinear form. An R-lattice M is called *even* if $x^2 = x \cdot x \in 2R$ for $x \in M$, where $x \cdot y\,(x,\, y \in M)$ is the associated bilinear form of M. If $R = \boldsymbol{Z}_p$ for odd p, the every R-lattice is even, so this terminology is meaningful only for $R = \boldsymbol{Z}$ and $\boldsymbol{Z}_2$.

A *finite symmetric bilinear form* means $\boldsymbol{Q}/\boldsymbol{Z}$-valued symmetric bilinear form on a finite abelian group. Let G be a finite abelian group. A map $q : G \longrightarrow \boldsymbol{Q}/2\boldsymbol{Z}$ is called a *finite quadratic form* on G if the following two conditions are satisfied:

i) $q(nx) = n^2 q(x)$ for $n \in \boldsymbol{Z},\, x \in G$;

ii) $q(x+y) - q(x) - q(y) = \langle 2 \rangle\, b(x,y)$ for $x,\, y \in G$,

where $\langle 2 \rangle$ is the isomorphism of $\boldsymbol{Q}/\boldsymbol{Z}$ onto $\boldsymbol{Q}/2\boldsymbol{Z}$ induced by the multiplication by 2 and b is a symmetric bilinear form on G; b is then called the *bilinear form associated with q*.

These forms on a finite abelian p-group can be considered to be $\boldsymbol{Q}_p/\boldsymbol{Z}_p$ or $\boldsymbol{Q}_2/2\boldsymbol{Z}_2$-valued, by the natural inclutions:

$$\boldsymbol{Q}_p/\boldsymbol{Z}_p \hookrightarrow \boldsymbol{Q}/\boldsymbol{Z} \quad \text{and} \quad \boldsymbol{Q}_2/2\boldsymbol{Z}_2 \hookrightarrow \boldsymbol{Q}/2\boldsymbol{Z}.$$

Let M be an R-lattice. We can consider a canonical embedding $M \hookrightarrow M^* = \mathrm{Hom}_R(M, R)$ determined by the nondegenerate bilinear form of M. We can extend the bilinear form of M to M^* as the restriction of the Q-valued extension on $M \otimes_R Q = M^* \otimes_R Q$, and we denote this form also by $x \cdot y\,(x,\, y \in M^*)$. The factor group $A = M^*/M$ is obviously finite. Now there is the unique finte bilinear form $b_M : A \times A \longrightarrow Q/R$ with

$$b_M(x+M, y+M) = x \cdot y + R \quad \text{for } x,\, y \in M^*.$$

Similarly when M is even, there is the unique finite quadratic form $q_M : A \longrightarrow Q/2R$ having b_M as its bilinear form and satisfying

$$q_M(x+M) = x^2 + 2R \quad \text{for } x \in M^*.$$

We call b_M the *discriminant bilinear form* of M, and q_M the *discriminant quadratic form* of M.

For an R-lattice M, the *discriminant* of M denoted by $\mathrm{discr}\, M$ is defined by $\mathrm{discr}\, M := \det(e_i, e_j) \pmod{(R^\times)^2}$, where $\{e_j\}$ is some basis of M (where $R^\times$

is the multiplicative group consist of all uints of R, and $(R^{\times})^2$ is the subgroup of squares). If $\operatorname{discr} M \in R^{\times}/(R^{\times})^2$, we say M is *unimodular*.

Let $\mathrm{Qu}(R)$ and $\mathrm{Qu}^+(R)$ be the semigroup of isomorphism classes of R-lattices and even R-lattices respectively, under the orthogonal direct sum. We denote the semigroup of finite symmetric bilinear forms and finite quadratic forms under $\oplus$, by $\mathrm{bil}(\boldsymbol{Z})$ and $\mathrm{qu}(\boldsymbol{Z})$ respectively. This notation is justified by the fact that the natural maps of $\mathrm{Qu}(\boldsymbol{Z})$, $\mathrm{Qu}^+(\boldsymbol{Z})$ to these groups are surjective. Corresponding to natural orthogonal direct sum decompositions

$$b_M = \bigoplus_p b_{M_p} \quad \text{and} \quad q_M = \bigoplus_p q_{M_p}$$

where $M_p \simeq M \otimes_{\boldsymbol{Z}} \boldsymbol{Z}_p$, we have the orthogonal direct sum decompositions

$$\mathrm{bil}(\boldsymbol{Z}) = \bigoplus_p \mathrm{bil}(\boldsymbol{Z}_p) \quad \text{and} \quad \mathrm{qu}(\boldsymbol{Z}) = \bigoplus_p \mathrm{qu}(\boldsymbol{Z}_p)$$

coming from the decomposition of a finite abelian group into its p-components. Consequently

$$\mathrm{Qu}(\boldsymbol{Z}_p) \longrightarrow \mathrm{bil}(\boldsymbol{Z}_p) \quad \text{and} \quad \mathrm{Qu}^+(\boldsymbol{Z}_p) \longrightarrow \mathrm{qu}(\boldsymbol{Z}_p)$$

are also surjective for each p.

Let M_1, $M_2 \in \mathrm{Qu}(\boldsymbol{Z})$ ($\mathrm{Qu}^+(\boldsymbol{Z})$ respectively), we say M_1 and M_2 are *stably equivalent* if there exist unimodular U_1, $U_2 \in \mathrm{Qu}(\boldsymbol{Z})$ ($\mathrm{Qu}^+(\boldsymbol{Z})$) such that $U_1 \oplus M_1 \simeq U_2 \oplus M_2$. With respect to this equivalence relation we denote the semigroup of equivalence classes of $\boldsymbol{Z}$-lattices by $\mathrm{St.Qu}(\boldsymbol{Z})$ and that of even $\boldsymbol{Z}$-lattices by $\mathrm{St.Qu}^+(\boldsymbol{Z})$. Now we can consider the two epimorphisms

$$b : \mathrm{St.Qu}(\boldsymbol{Z}) \longrightarrow \mathrm{bil}(\boldsymbol{Z}) \quad \text{and} \quad q : \mathrm{St.Qu}^+(\boldsymbol{Z}) \longrightarrow \mathrm{qu}(\boldsymbol{Z})$$

induced by the above natural mappings since the discriminant forms are trivial for unimodular lattices. It is proved that they are monomorphisms, so isomorphisms.

For any $\boldsymbol{Z}$-lattice M of signature $(t_{(+)}, t_{(-)})$, we define $\operatorname{sgn} M := t_{(+)} - t_{(-)} \pmod 8$. We call $\operatorname{sgn} M$ the *signature mod 8* of M, since danger of confusion might somehow be avoidable. It induces then the canonical homomorphism $\operatorname{sgn} : \mathrm{St.Qu}^+(\boldsymbol{Z}) \longrightarrow \boldsymbol{Z}/8\boldsymbol{Z}$ since the signature mod 8 is 0 for even unimodular $\boldsymbol{Z}$-lattice, and $\operatorname{sgn} : \mathrm{qu}(\boldsymbol{Z}) \longrightarrow \boldsymbol{Z}/8\boldsymbol{Z}$ via the above isomorphism q. We call $\operatorname{sgn} q$ for $q \in \mathrm{qu}(\boldsymbol{Z})$ also the *signature* of q. As is mentioned in the introduction, our objective is to give an explicit formula to this $\operatorname{sgn} : \mathrm{qu}(\boldsymbol{Z}) \longrightarrow \boldsymbol{Z}/8\boldsymbol{Z}$.

Following results are well known (cf. [1] Theorem 9.2).

The semigroup $\mathrm{Qu}(\boldsymbol{Z}_p)$ is generated by $K_\theta^{(p)}(p^k)$ for every odd p, and $\mathrm{Qu}(\boldsymbol{Z}_2)$ is generated by $K_\theta^{(2)}(2^k)$ and $U^{(2)}(2^k)$, and $V^{(2)}(2^k)$, where $K_\theta^{(p)}(p^k)$ is the p-adic lattice of rank 1 determined by the matrix (θp^k) $(k \geq 0,\ \theta \in \boldsymbol{Z}_p^{\times}/(\boldsymbol{Z}_p^{\times})^2)$ for all p, $U^{(2)}(2^k)$ and $V^{(2)}(2^k)$ are the 2-adic lattices of rank 2 determined by the matrices

$$\begin{pmatrix} 0 & 2^k \\ 2^k & 0 \end{pmatrix}, \quad \begin{pmatrix} 2^{k+1} & 2^k \\ 2^k & 2^{k+1} \end{pmatrix} \qquad (k \geq 0).$$

Thus the semigroup $\mathrm{qu}(\boldsymbol{Z})$ is generated by the discriminant quadratic forms of $K_\theta^{(p)}(p^k)$, $U^{(2)}(2^k)$ and $V^{(2)}(2^k)$ denoted by $q_\theta^{(p)}(p^k)$, $u_+^{(2)}(2^k)$ and $v_+^{(2)}(2^k)$, respectively, where $k \geq 1$. The semigroup bil($\boldsymbol{Z}$) is generated by the bilinear forms of $q_\theta^{(p)}(p^k)$, $u_+^{(2)}(2^k)$ and $v_+^{(2)}(2^k)$ denoted by $b_\theta^{(p)}(p^k)$, $u_-^{(2)}(2^k)$ and $v_-^{(2)}(2^k)$, respectively, where $k \geq 1$.

1.2 The Hilbert symbol and the Jacobi symbol

In this section we introduce the Hilbert and Jacobi symbols and we mention some of thier properties which we use in later discussions.

Let $m = \pm \prod_i p_i^{e_i}$ be an odd integer (where p_i's are prime numbers and e_i's are positive integers). If n is an integer with $(m, n) = 1$, then the *Jacobi symbol* is defined by

$$\left(\frac{n}{m}\right) := \prod_i \left(\frac{n}{p_i}\right)^{e_i}, \tag{1}$$

where $\left(\frac{n}{p_i}\right)$ is the Legendre symbol.

Let $V := \{v \mid v \text{ is a prime number or } v = \infty\}$, i.e., the set of valuations on $\boldsymbol{Q}$, and let

$$F_v := \begin{cases} \boldsymbol{Q}_p & \text{if } v = p \text{ :prime,} \\ \boldsymbol{R} & \text{if } v = \infty. \end{cases}$$

For $a, b \in F_v^\times = F_v \setminus \{0\}$, we define the *Hilbert symbol* $(a, b)_v$ letting it be 1 or -1 according as the F_v-inner product space given by the diagonal matrix $[a, b, -1]$ is isotropic or not.

The Hilbert symbol is computed explicitly as follows (see [3]):
For $a, b \in F_\infty^\times = \boldsymbol{R}^\times$,

$$(a, b)_\infty = \begin{cases} 1 & \text{if } a > 0 \text{ or } b > 0, \\ -1 & \text{if } a < 0 \text{ and } b < 0. \end{cases} \tag{2}$$

If $a = p^\alpha a'$, and $b = p^\beta b'$ are in $F_p^\times = \boldsymbol{Q}_p^\times$ for a prime p, where a', $b' \in \boldsymbol{Z}_p^\times$, α and β are non-negative integers. Then

$$(a, b)_p = (-1)^{\alpha\beta\epsilon(p)} \left(\frac{a'}{p}\right)^\beta \left(\frac{b'}{p}\right)^\alpha \quad \text{for } p \neq 2, \tag{3}$$

$$(a, b)_2 = (-1)^{\epsilon(a')\epsilon(b') + \alpha\omega(b') + \beta\omega(a')} \tag{4}$$

where $\epsilon(z) \equiv \frac{z-1}{2} \pmod 2$, $\omega(z) \equiv \frac{z^2-1}{8} \pmod 2$. Thus $(\ ,\ )_v$ is multiplicatively bilinear and we have the product formula

$$\prod_{v \in V} (a, b)_v = 1 \quad \text{for } a, b \in \boldsymbol{Q}^\times. \tag{5}$$

Let m and n be integers with m odd and $(m, n) = 1$. Then

$$\left(\frac{n}{m}\right) = \prod_{p \mid m} (m, n)_p. \tag{6}$$

In fact, if $m = p^\alpha u$, where α is positive integer and $p \nmid u$, i.e., $u \in \boldsymbol{Z}_p^\times$ then $n \in \boldsymbol{Z}_p^\times$ since $(m,n) = 1$. By (3), $(m,n)_p = \left(\frac{n}{p}\right)^\alpha$ ($p \neq 2$ because m is odd integer). Hence (6) holds by the definition (1).

Let m and n are odd integers with $(m,n) = 1$. $(m,n)_2 = (-1)^{\epsilon(m)\epsilon(n)}$ by (4). $(m,n)_p = 1$ for $p \nmid mn$ by (3), and by (5),

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (m,n)_\infty(-1)^{\epsilon(m)\epsilon(n)}. \tag{7}$$

For odd integer n,

$$\left(\frac{2}{n}\right) = (-1)^{\omega(n)} \tag{8}$$

since $\left(\frac{2}{p}\right) = (-1)^{\omega(p)}$ for any odd prime p.

Let n be an odd integer and m be an integer with $(m,n) = 1$. If an integer m' satisfies $m \equiv m' \pmod n$ then by the definition (1),

$$\left(\frac{m}{n}\right) = \left(\frac{m'}{n}\right). \tag{9}$$

2 The signature of the discriminant forms

We calculate the signature for the generators of $\mathrm{qu}(\boldsymbol{Z})$ mentioned in Sec. 1.1. We deal with the case where p is odd in the first part ($q_\theta^{(p)}(p^k)$), and the case where p is even in the second ($q_\theta^{(2)}(2^k)$). In the last two parts we include also a treatment of some exceptional cases for the completeness ($u_+^{(2)}(2^k)$ and $v_+^{(2)}(2^k)$). See [4].

2.1 The signature of $q_\theta^{(p)}(p^k)$ for odd p

The purpose of this section is to prove the following formula:

$$\operatorname{sgn} q_\theta^{(p)}(p^k) \equiv k^2(1-p) + 4k\eta \pmod 8 \tag{10}$$

for odd prime p, $\theta \in \boldsymbol{Z}_p^\times/(\boldsymbol{Z}_p^\times)^2$ and $0 < k \in \boldsymbol{Z}$. Here η satisfies $\left(\frac{\theta}{p}\right) = (-1)^\eta$.

The proof is given as follows:

Using the method of [4], we can construct an even $\boldsymbol{Z}$-lattice with discriminant quadratic form $q_\theta^{(p)}(p^k)$ as follows. We can take $2n$ for a representative of θ, where $n \in \boldsymbol{Z}$. To begin with, we take $d_1, d_2 \in \boldsymbol{Z}$ such that $d_1 \equiv 0 \pmod 2$, $d_2 \equiv 1 \pmod 2$ and that

$$1 = 2nd_1 - p^k d_2. \tag{11}$$

There exist then $a_1, d_3 \in \boldsymbol{Z}$ satisfying $a_1 \equiv 0 \pmod 2$, $|d_3| < |d_2|$ and

$$d_1 = a_1 d_2 - d_3. \tag{12}$$

If d_3 is not 0, we can do the same thing by replacing d_1, d_2 by d_2, d_3. We will repeat this division process as far as possible. We obtain successively a_{j-1}, $d_{j+1} \in \boldsymbol{Z}$ satisfying $a_{j-1} \equiv 0 \pmod 2$, $|d_{j+1}| < |d_j|$ and

$$d_{j-1} = a_{j-1}d_j - d_{j+1} \tag{13}$$

for $j = 2, 3, \ldots$. We have

$$d_1 \equiv d_3 \equiv \cdots \equiv d_{2j-1} \equiv \cdots \equiv 0 \pmod 2, \tag{14}$$
$$d_2 \equiv d_4 \equiv \cdots \equiv d_{2j} \equiv \cdots \equiv 1 \pmod 2 \tag{15}$$

and there exists r such that $d_{2r} = \pm 1$,

$$d_{2r-2} = a_{2r-2}d_{2r-1} - d_{2r} \quad (a_{2r-2} \equiv 0 \pmod 2),\ |d_{2r}| < |d_{2r-1}|) \tag{16}$$

and that

$$d_{2r-1} = a_{2r-1}d_{2r} \quad (a_{2r-1} \equiv 0 \pmod 2)). \tag{17}$$

This process ends at this stage.

Putting $d_0 := 1/p^r$ and $a_0 := 2n/p^r$, we now introduce the matrices $L \in \mathrm{M}_{2r}(\boldsymbol{Q})$ and $M \in \mathrm{M}_{2r}(\boldsymbol{Z})$ by

$$L := \begin{pmatrix} a_0 & 1 & 0 & \ldots & 0 & 0 \\ 1 & a_1 & 1 & \ldots & 0 & 0 \\ 0 & 1 & a_2 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & a_{2r-2} & 1 \\ 0 & 0 & 0 & \ldots & 1 & a_{2r-1} \end{pmatrix},$$

$$M := \begin{pmatrix} 2np^k & p^k & 0 & \ldots & 0 & 0 \\ p^k & a_1 & 1 & \ldots & 0 & 0 \\ 0 & 1 & a_2 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & a_{2r-2} & 1 \\ 0 & 0 & 0 & \ldots & 1 & a_{2r-1} \end{pmatrix}.$$

Then $\det L = 1/p^k$ and $\det M = p^k$. In fact, we can see that in L, the determinant of the last i rows and columns is d_{2r-i} by induction on i, hence by (11)

$$\det L = a_0 d_1 - d_2 = p^{-k}(2nd_1 - p^k d_2) = p^{-k},$$

hence $\det M = p^k$. The matrix M defines in a usual way the even $\boldsymbol{Z}$-lattce, denoted by the same letter M. Then we see that the discriminant quadratic form of M is $q_\theta^{(p)}(p^k)$. In fact, the class of ${}^t(p^{-k}, 0, \ldots, 0)$ generates the group M^*/M and we have

$$(p^{-k}, 0, \ldots, 0)M^t(p^{-k}, 0, \ldots, 0) = 2np^{-k}.$$

The signature of M is equal to that of L, so we shall calculate the signature mod 8 of L. We will first diagonalize the symmetric matrix L by giving the following basis:

$$f_1 = \begin{pmatrix} d_1 \\ -d_2 \\ d_3 \\ -d_4 \\ \vdots \\ d_{2r-1} \\ -d_{2r} \end{pmatrix}, \ f_2 = \begin{pmatrix} 0 \\ -d_2 \\ d_3 \\ -d_4 \\ \vdots \\ d_{2r-1} \\ -d_{2r} \end{pmatrix}, \ f_3 = \begin{pmatrix} 0 \\ 0 \\ d_3 \\ -d_4 \\ \vdots \\ d_{2r-1} \\ -d_{2r} \end{pmatrix}, \ldots .$$

Since

$$Lf_1 = \begin{pmatrix} d_0 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ Lf_2 = \begin{pmatrix} -d_2 \\ -d_1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ Lf_3 = \begin{pmatrix} 0 \\ d_3 \\ d_2 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots ,$$

we obtain

$$ {}^t f_i L f_j = \begin{cases} d_{i-1}d_i & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases} \tag{18}$$

Thus

$$L \sim \begin{pmatrix} d_0d_1 & & & & \\ & d_1d_2 & & \text{\huge 0} & \\ & & \ddots & & \\ & \text{\huge 0} & & d_{2r-2}d_{2r-1} & \\ & & & & d_{2r-1}d_{2r} \end{pmatrix}. \tag{19}$$

We put now

$$\begin{aligned} \delta_{2j-1} &:= (-1)^{j-1} d_{2j-1}, \\ \delta_{2j} &:= (-1)^j d_{2j}, \\ \alpha_j &:= (-1)^j a_j/2 \end{aligned} \tag{20}$$

and rewrite (13) as follows:

$$\delta_{2j-2} = 2\alpha_{2j-2}\delta_{2j-1} + \delta_{2j}, \tag{21}$$
$$\delta_{2j-1} = 2\alpha_{2j-1}\delta_{2j} + \delta_{2j+1}. \tag{22}$$

Since $\delta_{2j-1} \equiv 0 \pmod 2$ by (14), we have

$$\delta_2 \equiv \delta_4 \equiv \cdots \equiv \delta_{2r} \pmod 4$$

by (21). The equality (11) shows $p^k(-d_2) \equiv 1 \pmod 4$, i.e., $-d_2 \equiv p^k \pmod 4$. Note that

$$p \equiv (-1)^{\epsilon(p)} \pmod 4.$$

Hence

$$\delta_{2j} \equiv \delta_2 \equiv -d_2 \equiv p^k \equiv (-1)^{k\epsilon(p)} \pmod 4.$$

In particular,

$$d_{2r} = (-1)^r \delta_{2r} \equiv (-1)^{r+k\epsilon(p)} \pmod 4.$$

Consequently, since $d_{2r} = \pm 1$,

$$d_{2r} = (-1)^{r+k\epsilon(p)}. \tag{23}$$

We define $\delta'_{2j-1}, \delta''_{2j-1}, m_j \in \boldsymbol{Z}$ $(m_j \geq 0)$ as follows:

$$\begin{aligned} \delta_{2j-1} &= 2\delta'_{2j-1}, \\ \delta'_{2j-1} &= 2^{m_j}\delta''_{2j-1}, \\ \delta''_{2j-1} &\equiv 1 \pmod 2. \end{aligned} \tag{24}$$

Now, because (21) can be rewritten to $\delta_{2j-2} = 2^{m_j+2}\alpha_{2j-2}\delta''_{2j-1} + \delta_{2j}$,

$$\left(\frac{\delta_{2j-2}}{\delta''_{2j-1}}\right) = \left(\frac{\delta_{2j}}{\delta''_{2j-1}}\right), \text{ i.e., } \left(\frac{\delta_{2j-2}}{\delta''_{2j-1}}\right)\left(\frac{\delta_{2j}}{\delta''_{2j-1}}\right) = 1.$$

The reciprocity (7) implies

$$\begin{aligned} &\left(\frac{\delta''_{2j-1}}{\delta_{2j-2}}\right)\left(\frac{\delta''_{2j-1}}{\delta_{2j}}\right) \\ &= \left(\frac{\delta''_{2j-1}}{\delta_{2j-2}}\right)\left(\frac{\delta''_{2j-1}}{\delta_{2j}}\right)\left(\frac{\delta_{2j-2}}{\delta''_{2j-1}}\right)\left(\frac{\delta_{2j}}{\delta''_{2j-1}}\right) \\ &= (\delta''_{2j-1}, \delta_{2j-2})_\infty(\delta''_{2j-1}, \delta_{2j})_\infty(-1)^{\epsilon(\delta_{2j-2})\epsilon(\delta''_{2j-1})+\epsilon(\delta_{2j})\epsilon(\delta''_{2j-1})} \\ &= (\delta_{2j-2}, \delta''_{2j-1})_\infty(\delta''_{2j-1}, \delta_{2j})_\infty \\ &= (\delta_{2j-2}, \delta_{2j-1})_\infty(\delta_{2j-1}, \delta_{2j})_\infty. \end{aligned} \tag{25}$$

The Jacobi symbol $\left(\frac{2^{m_j}}{\delta_{2j-2}}\right)$ is equal to $\left(\frac{2^{m_j}}{\delta_{2j}}\right)$, i.e.,

$$\left(\frac{2^{m_j}}{\delta_{2j-2}}\right)\left(\frac{2^{m_j}}{\delta_{2j}}\right) = 1. \tag{26}$$

This is obvious when $m_j = 0$. If $m_j > 0$, then $\delta_{2j-2} \equiv \delta_{2j} \pmod 8$ by $\delta_{2j-1} \equiv 0 \pmod 4$ and (21). This proves $\left(\frac{2}{\delta_{2j-2}}\right) = \left(\frac{2}{\delta_{2j}}\right)$ by (8). Hence (26) holds, also in this case.

By (25) and (26), we obtain

$$\left(\frac{\delta'_{2j-1}}{\delta_{2j-2}}\right)\left(\frac{\delta'_{2j-1}}{\delta_{2j}}\right) = (\delta_{2j-2}, \delta_{2j-1})_\infty(\delta_{2j-1}, \delta_{2j})_\infty. \tag{27}$$

By (22), $\delta'_{2j-1} = \alpha_{2j-1}\delta_{2j} + \delta'_{2j+1}$. It follows that

$$\left(\frac{\delta'_{2j-1}}{\delta_{2j}}\right) = \left(\frac{\delta'_{2j+1}}{\delta_{2j}}\right). \tag{28}$$

By this, (27) is equivalent to

$$\left(\frac{\delta'_{2j-1}}{\delta_{2j-2}}\right)\left(\frac{\delta'_{2j+1}}{\delta_{2j}}\right) = (\delta_{2j-2},\delta_{2j-1})_\infty(\delta_{2j-1},\delta_{2j})_\infty. \tag{29}$$

We have $\left(\frac{\delta'_{2r-1}}{\delta_{2r}}\right) = 1$ since $\delta_{2r} = \pm 1$, so (27) is, in case $j = r$, of the form

$$\left(\frac{\delta'_{2r-1}}{\delta_{2r-2}}\right) = (\delta_{2r-2},\delta_{2r-1})_\infty(\delta_{2r-1},\delta_{2r})_\infty.$$

We write (29) separately:

$$\begin{aligned}
\left(\frac{\delta'_{2r-3}}{\delta_{2r-4}}\right)\left(\frac{\delta'_{2r-1}}{\delta_{2r-2}}\right) &= (\delta_{2r-4},\delta_{2r-3})_\infty(\delta_{2r-3},\delta_{2r-2})_\infty,\\
&\ \vdots\\
\left(\frac{\delta'_{2j-1}}{\delta_{2j-2}}\right)\left(\frac{\delta'_{2j+1}}{\delta_{2j}}\right) &= (\delta_{2j-2},\delta_{2j-1})_\infty(\delta_{2j-1},\delta_{2j})_\infty,\\
&\ \vdots\\
\left(\frac{\delta'_{5}}{\delta_{4}}\right)\left(\frac{\delta'_{7}}{\delta_{6}}\right) &= (\delta_{4},\delta_{5})_\infty(\delta_{5},\delta_{6})_\infty,\\
\left(\frac{\delta'_{3}}{\delta_{2}}\right)\left(\frac{\delta'_{5}}{\delta_{4}}\right) &= (\delta_{2},\delta_{3})_\infty(\delta_{3},\delta_{4})_\infty.
\end{aligned}$$

Further, by applying (28) to $j = 1$, we have

$$\left(\frac{\delta'_1}{\delta_2}\right) = \left(\frac{\delta'_3}{\delta_2}\right).$$

Thus we obtain

$$\begin{aligned}
\left(\frac{\delta'_1}{\delta_2}\right) &= \prod_{j=2}^{2r-1}(\delta_j,\delta_{j+1})_\infty\\
&= (\delta_2,\delta_3)_\infty(\delta_3,\delta_4)_\infty\cdots(\delta_{2r-1},\delta_{2r})_\infty
\end{aligned} \tag{30}$$

by multiplying above equalities. To deduce the desired formula

$$\begin{aligned}
\left(\frac{n}{p^k}\right) &= \prod_{j=1}^{2r-1}(\delta_j,\delta_{j+1})_\infty\\
&= (\delta_1,\delta_2)_\infty(\delta_2,\delta_3)_\infty\cdots(\delta_{2r-1},\delta_{2r})_\infty,
\end{aligned} \tag{31}$$

still we have to prove

$$\left(\frac{\delta'_1}{\delta_2}\right) = (\delta_1,\delta_2)_\infty\left(\frac{n}{p^k}\right) \tag{32}$$

which is shown as follows:
Note first that $\left(\frac{\delta_2}{\delta''_1}\right)\left(\frac{p^k}{\delta''_1}\right) = 1$, $\epsilon(\delta_2) = \epsilon(p^k)$ which follow from $1 = 4n\delta'_1 + p^k\delta_2$,

$\delta_2 \equiv p^k \pmod 4$. By a similar way as in proving (26), $\left(\frac{2^{m_1}}{\delta_2}\right)\left(\frac{2^{m_1}}{p^k}\right) = 1$. Combining these,

$$\begin{aligned}
\left(\frac{\delta_1'}{\delta_2}\right)\left(\frac{\delta_1'}{p^k}\right) &= \left(\frac{2^{m_1}}{\delta_2}\right)\left(\frac{2^{m_1}}{p^k}\right)\left(\frac{\delta_1''}{\delta_2}\right)\left(\frac{\delta_1''}{p^k}\right) \\
&= \left(\frac{\delta_1''}{\delta_2}\right)\left(\frac{\delta_1''}{p^k}\right)\left(\frac{\delta_2}{\delta_1''}\right)\left(\frac{p^k}{\delta_1''}\right) \\
&= (\delta_1'', \delta_2)_\infty (\delta_1'', p^k)_\infty (-1)^{\epsilon(\delta_1'')\epsilon(\delta_2)+\epsilon(\delta_1'')\epsilon(p^k)} \\
&= (\delta_1'', \delta_2)_\infty \\
&= (\delta_1, \delta_2)_\infty .
\end{aligned}$$

On the other hand $\left(\frac{\delta_1'}{p^k}\right)\left(\frac{n}{p^k}\right) = \left(\frac{4n\delta_1'}{p^k}\right) = \left(\frac{1}{p^k}\right) = 1$, i.e.,

$$\left(\frac{\delta_1'}{p^k}\right) = \left(\frac{n}{p^k}\right).$$

Thus we proved (32), so established also (31).

Now the terms of the product in (31) are rewritten as follows:

$$\begin{aligned}
(\delta_1, \delta_2)_\infty &= (d_1, -d_2)_\infty \\
&= (-1, d_1)_\infty (d_1, d_2)_\infty , \\
&\vdots \\
(\delta_{2j-1}, \delta_{2j})_\infty &= ((-1)^{j-1} d_{2j-1}, (-1)^j d_{2j})_\infty \\
&= (-1)^{(j-1)j} (-1, d_{2j-1})_\infty^j (-1, d_{2j})_\infty^{j-1} (d_{2j-1}, d_{2j})_\infty \\
&= (-1, d_{2j-1})_\infty^j (-1, d_{2j})_\infty^{j-1} (d_{2j-1}, d_{2j})_\infty , \\
(\delta_{2j}, \delta_{2j+1})_\infty &= ((-1)^j d_{2j}, (-1)^j d_{2j+1})_\infty \\
&= (-1)^j (-1, d_{2j})_\infty^j (-1, d_{2j+1})_\infty^j (d_{2j}, d_{2j+1})_\infty , \\
&\vdots \\
(\delta_{2r-1}, \delta_{2r})_\infty &= ((-1)^{r-1} d_{2r-1}, (-1)^r d_{2r})_\infty \\
&= (-1, d_{2r-1})_\infty^r (-1, d_{2r})_\infty^{r-1} (d_{2r-1}, d_{2r})_\infty .
\end{aligned}$$

Furthermore, by (23), we have

$$(-1, d_{2r})_\infty^{r-1} = (-1, (-1)^{r+k\epsilon(p)})_\infty^{r-1} = (-1)^{(r-1)k\epsilon(p)}. \tag{33}$$

By multiplying these, we see that (31) is now of the form

$$\left(\frac{n}{p^k}\right) = (-1)^{(r-1)r/2+(r-1)k\epsilon(p)} (-1, d_1 d_2 \ldots d_{2r-1})_\infty \prod_{j=1}^{2r-1} (d_j, d_{j+1})_\infty . \tag{34}$$

On the other hand, we recall that $2n$ is a representative of θ and the definition of η, we obtain

$$\left(\frac{n}{p^k}\right) = \left(\frac{2}{p^k}\right)\left(\frac{2n}{p^k}\right) = (-1)^{k\omega(p)+k\eta}. \tag{35}$$

A simple computation gives

$$\prod_{0\le i<j\le 2r-1}(d_id_{i+1},d_jd_{j+1})_\infty=(-1,d_1d_2\dots d_{2r-1})_\infty\prod_{j=1}^{2r-1}(d_j,d_{j+1})_\infty. \tag{36}$$

Now, with the signature $(t_{(+)},t_{(-)})$ of L, we have $t_{(+)}+t_{(-)}=2r$ and

$$\begin{aligned}(-1)^{t_{(-)}(t_{(-)}-1)/2} &= \prod_{0\le i<j\le 2r-1}(d_id_{i+1},d_jd_{j+1})_\infty && \text{(by (2))}\\ &= (-1,d_1d_2\dots d_{2r-1})_\infty\prod_{j=1}^{2r-1}(d_j,d_{j+1})_\infty && \text{(by (36))}\\ &= \left(\frac{n}{p^k}\right)(-1)^{(r-1)r/2+(r-1)k\epsilon(p)} && \text{(by (34))}\\ &= (-1)^{(r-1)r/2+(r-1)k\epsilon(p)+k\omega(p)+k\eta}. && \text{(by (35))}\end{aligned}$$

Multiplying diagonal elements in (19), and (23), we get

$$(-1)^{t_{(-)}}=(-1)^{r+k\epsilon(p)}. \tag{37}$$

Note $(-1)^m\equiv 1+2m \pmod 4$, so

$$2(-1)^m\equiv 2(1+2m)\pmod 8. \tag{38}$$

We have also

$$(-1)^m\equiv 1-2m^2\pmod 8, \tag{39}$$

$$4m\equiv 4m^2\pmod 8. \tag{40}$$

Hence

$$\begin{aligned}-2t_{(-)} &= 2\{1+2(t_{(-)}-1)t_{(-)}/2\}+1-2t_{(-)}^2-3\\ &\equiv 2(-1)^{(t_{(-)}-1)t_{(-)}/2}+(-1)^{t_{(-)}}-3\\ &\equiv 2(-1)^{(r-1)r/2+(r-1)k\epsilon(p)+k\omega(p)+k\eta}+(-1)^{r+k\epsilon(p)}-3\\ &\equiv 2\{1+2((r-1)r/2+(r-1)k\epsilon(p)+k\omega(p)+k\eta)\}\\ &\quad +1-2(r+k\epsilon(p))^2-3\\ &\equiv 2(r-1)r+4(r-1)k\epsilon(p)+4k\omega(p)+4k\eta\\ &\quad -2r^2-4rk\epsilon(p)-2k^2\epsilon(p)^2\\ &\equiv 2(r-1)r+4(r-1)k^2\epsilon(p)+4k^2\omega(p)+4k\eta\\ &\quad -2r^2-4rk^2\epsilon(p)-2k^2\epsilon(p)^2\\ &\equiv -2r+k^2(-4\epsilon(p)+4\omega(p)-2\epsilon(p)^2)+4k\eta\\ &\equiv -2r+k^2(1-p)+4k\eta\end{aligned}$$

modulo 8; that is,

$$2r-2t_{(-)}\equiv k^2(1-p)+4k\eta\pmod 8.$$

Since the left hand side is obviously the signature mod 8 of L, we have thus proved the desired formula (10).

2.2 The signature of $q_\theta^{(2)}(2^k)$

In this section, we will prove the following supplementary formula

$$\operatorname{sgn} q_\theta^{(2)}(2^k) \equiv \theta + 4\omega(\theta)k \pmod 8 \tag{41}$$

where $\theta \in \boldsymbol{Z}_2^\times/(\boldsymbol{Z}_2^\times)^2$ and $0 < k \in \boldsymbol{Z}$. This is of the equal importance.

To begin with, we can take an odd integer n for a representative of θ. The proof is similar to that of $q_\theta^{(p)}(p^k)$ in previous section 2.1. We take $d_1, d_2 \in \boldsymbol{Z}$ such that $d_1 \equiv 1 \pmod 2$, $d_2 \equiv 0 \pmod 2$ and that

$$1 = nd_1 - 2^k d_2. \tag{42}$$

By the same division process as in 2.1, we can find $a_{j-1}, d_{j+1} \in \boldsymbol{Z}$ satisfying $a_{j-1} \equiv 0 \pmod 2$, $|d_{j+1}| < |d_j|$ and

$$d_{j-1} = a_{j-1}d_j - d_{j+1} \tag{43}$$

for $j = 2, 3, \ldots$. This time we have

$$d_1 \equiv d_3 \equiv \cdots \equiv d_{2j-1} \equiv \cdots \equiv 1 \pmod 2, \tag{44}$$

$$d_2 \equiv d_4 \equiv \cdots \equiv d_{2j} \equiv \cdots \equiv 0 \pmod 2 \tag{45}$$

and there exists r such that $d_{2r-1} = \pm 1$,

$$d_{2r-3} = a_{2r-3}d_{2r-2} - d_{2r-1} \quad (a_{2r-3} \equiv 0 \pmod 2),\ |d_{2r-1}| < |d_{2r-2}|) \tag{46}$$

and that

$$d_{2r-2} = a_{2r-2}d_{2r-1} \quad (a_{2r-2} \equiv 0 \pmod 2)). \tag{47}$$

With $d_0 := 1/2^r$ and $a_0 := n/2^r$. The matrix $L \in \mathrm{M}_{2r-1}(\boldsymbol{Q})$ is given now by

$$L := \begin{pmatrix} a_0 & 1 & 0 & \ldots & 0 & 0 \\ 1 & a_1 & 1 & \ldots & 0 & 0 \\ 0 & 1 & a_2 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & a_{2r-3} & 1 \\ 0 & 0 & 0 & \ldots & 1 & a_{2r-2} \end{pmatrix}.$$

In the same way as in 2.1, we see that the signature mod 8 of L is equal to $\operatorname{sgn} q_\theta^{(2)}(2^k)$. Similarly, we can show

$$L \sim \begin{pmatrix} d_0d_1 & & & & 0 \\ & d_1d_2 & & & \\ & & \ddots & & \\ 0 & & & d_{2r-3}d_{2r-2} & \\ & & & & d_{2r-2}d_{2r-1} \end{pmatrix}.$$

We use the same δ_j and α_j as in the definition (20):

$$\begin{aligned} \delta_{2j-1} &:= (-1)^{j-1}d_{2j-1}, \\ \delta_{2j} &:= (-1)^j d_{2j}, \\ \alpha_j &:= (-1)^j a_j/2. \end{aligned}$$

Then by (43),

$$\begin{aligned} \delta_{2j-2} &= 2\alpha_{2j-2}\delta_{2j-1} + \delta_{2j}, & (48)\\ \delta_{2j-1} &= 2\alpha_{2j-1}\delta_{2j} + \delta_{2j+1}. & (49) \end{aligned}$$

Since $\delta_{2j} \equiv 0 \pmod 2$ by (45). We have by (49),

$$\delta_1 \equiv \delta_3 \equiv \cdots \equiv \delta_{2r-1} \pmod 4.$$

From (42), $d_{2r-1} = \pm 1$ and $n \equiv (-1)^{\epsilon(n)} \pmod 4$, it follows

$$d_{2r-1} = (-1)^{r-1+\epsilon(n)}. \tag{50}$$

We introduce now the similar notation δ'_{2j}, δ''_{2j}, $m_j \in \boldsymbol{Z}$ $(m_j \geq 0)$:

$$\begin{aligned} \delta_{2j} &= 2\delta'_{2j},\\ \delta'_{2j} &= 2^{m_j}\delta''_{2j},\\ \delta''_{2j} &\equiv 1 \pmod 2). \end{aligned}$$

Instead of (27), we get

$$\left(\frac{\delta'_{2j-2}}{\delta_{2j-3}}\right)\left(\frac{\delta'_{2j-2}}{\delta_{2j-1}}\right) = (\delta_{2j-3}, \delta_{2j-2})_\infty(\delta_{2j-2}, \delta_{2j-1})_\infty. \tag{51}$$

Dividing (48) by 2, $\delta'_{2j-2} = \alpha_{2j-2}\delta_{2j-1} + \delta'_{2j}$. This implies that $\left(\frac{\delta'_{2j-2}}{\delta_{2j-1}}\right) = \left(\frac{\delta'_{2j}}{\delta_{2j-1}}\right)$. Now (51) is equivalent to

$$\left(\frac{\delta'_{2j-2}}{\delta_{2j-3}}\right)\left(\frac{\delta'_{2j}}{\delta_{2j-1}}\right) = (\delta_{2j-3}, \delta_{2j-2})_\infty(\delta_{2j-2}, \delta_{2j-1})_\infty. \tag{52}$$

By multiplying the sequence of equalities (52), we deduce

$$\left(\frac{\delta'_2}{\delta_1}\right) = \prod_{j=1}^{2r-2} (\delta_j, \delta_{j+1})_\infty. \tag{53}$$

As before, from (42), it follows that $\left(\frac{2^{m_1}}{n}\right)\left(\frac{2^{m_1}}{\delta_1}\right) = 1$ and $\left(\frac{n}{\delta''_2}\right)\left(\frac{\delta_1}{\delta''_2}\right) = 1$. (See the discussion before (26).) From these

$$\begin{aligned} \left(\frac{\delta'_2}{n}\right)\left(\frac{\delta'_2}{\delta_1}\right) &= \left(\frac{2^{m_1}}{n}\right)\left(\frac{2^{m_1}}{\delta_1}\right)\left(\frac{\delta''_2}{n}\right)\left(\frac{\delta''_2}{\delta_1}\right)\\ &= \left(\frac{\delta''_2}{n}\right)\left(\frac{\delta''_2}{\delta_1}\right)\\ &= \left(\frac{\delta''_2}{n}\right)\left(\frac{\delta''_2}{\delta_1}\right)\left(\frac{n}{\delta''_2}\right)\left(\frac{\delta_1}{\delta''_2}\right)\\ &= (\delta''_2, n\delta_1)_\infty\\ &= (2^k\delta_2, n\delta_1)_\infty\\ &= (1 - n\delta_1, n\delta_1)_\infty\\ &= 1. \end{aligned}$$

On the other hand $\left(\frac{\delta_2'}{n}\right)\left(\frac{2}{n}\right)^{k+1} = 1$ since $2^{k+1}\delta_2' \equiv 1 \pmod{n}$. Thus $\left(\frac{\delta_2'}{\delta_1}\right) = \left(\frac{\delta_2'}{n}\right) = \left(\frac{2}{n}\right)^{k+1}$. Now (53) is equivalent to

$$\left(\frac{2}{n}\right)^{k+1} = \prod_{j=1}^{2r-2} (\delta_j, \delta_{j+1})_\infty.$$

By (50), we have

$$(-1, d_{2r-1})_\infty = (-1)^{(r-1)^2+(r-1)\epsilon(n)}.$$

In the same way as in the proof of (34), we obtain

$$\left(\frac{2}{n}\right)^{k+1} = (-1)^{(r-2)(r-1)/2+(r-1)\epsilon(n)}(-1, d_1 d_2 \dots d_{2r-2})_\infty \prod_{j=1}^{2r-2} (d_j, d_{j+1})_\infty.$$

We have also a similar formula to (36):

$$\prod_{0 \le i < j \le 2r-2} (d_i d_{i+1}, d_j d_{j+1})_\infty = (-1, d_1 d_2 \dots d_{2r-2})_\infty \prod_{j=1}^{2r-2} (d_j, d_{j+1})_\infty.$$

By (2), the left hand side of this equality is equal to $(-1)^{t_{(-)}(t_{(-)}-1)/2}$ with the signature $(t_{(+)}, t_{(-)})$ of L. On the other hand $\left(\frac{2}{n}\right)^{k+1} = (-1)^{(k+1)\omega(n)}$ by (8). Combining these we obtain

$$(-1)^{t_{(-)}(t_{(-)}-1)/2} = (-1)^{(k+1)\omega(n)+(r-2)(r-1)/2+(r-1)\epsilon(n)}. \tag{54}$$

Instead of (37), we have by (50),

$$(-1)^{t_{(-)}} = (-1)^{r-1+\epsilon(n)}. \tag{55}$$

Using (54), (55), (38), (39) and (40),

$$\begin{aligned}
-2t_{(-)} &= 2\{1 + 2(t_{(-)} - 1)t_{(-)}/2\} + 1 - 2t_{(-)}^2 - 3 \\
&\equiv 2(-1)^{(t_{(-)}-1)t_{(-)}/2} + (-1)^{t_{(-)}} - 3 \\
&= (-1)^{(k+1)\omega(n)+(r-2)(r-1)/2+(r-1)\epsilon(n)} + (-1)^{r-1+\epsilon(n)} - 3 \\
&\equiv 2\{1 + 2((k+1)\omega(n) + (r-2)(r-1)/2 + (r-1)\epsilon(n))\} \\
&\quad +1 - 2(r - 1 + \epsilon(n))^2 - 3 \\
&\equiv -2r + 2 + 4k\omega(n) + 4\omega(n) - 2\epsilon(n)^2 \\
&\equiv -2r + 2 + 4k\omega(n) + n - 1
\end{aligned}$$

modulo 8. Thus

$$2r - 1 - 2t_{(-)} \equiv n + 4k\omega(n) \pmod{8}.$$

The left hand side is $t_{(+)} - t_{(-)}$ since $t_{(+)} + t_{(-)} = 2r - 1$. Since n was a representative of θ, we have establish the formula (41).

2.3 The signature of $u_+^{(2)}(2^k)$

To be complete, we add the following formula:

$$\operatorname{sgn} u_+^{(2)}(2^k) \equiv 0 \pmod 8, \qquad 0 < k \in \boldsymbol{Z}. \tag{56}$$

The proof is almost trivial. Let M be a $\boldsymbol{Z}$-lattice of rank 2, having basis $\{e_1, e_2\}$ with the inner product

$$\begin{pmatrix} e_1 \\ e_2 \end{pmatrix} (e_1, e_2) = \begin{pmatrix} 0 & 2^k \\ 2^k & 0 \end{pmatrix}.$$

Since $U^{(2)}(2^k) \simeq M \otimes_{\boldsymbol{Z}} \boldsymbol{Z}_2$ and $\det M$ is 2-power, we see that the discriminant form of M is exactly $u_+^{(2)}(2^k)$. We put now $\xi_1 := e_1 + e_2$, $\xi_2 := e_1 - e_2$. Then we have

$$\begin{pmatrix} \xi_1 \\ \xi_2 \end{pmatrix} (\xi_1, \xi_2) = \begin{pmatrix} 2^{k+1} & 0 \\ 0 & -2^{k+1} \end{pmatrix}.$$

Hence we conclude the signature of M is $(1, 1)$. From this it follows (56).

2.4 The signature of $v_+^{(2)}(2^k)$

The only remaining formula is now

$$\operatorname{sgn} v_+^{(2)}(2^k) \equiv 4k \pmod 8 \qquad 0 < k \in \boldsymbol{Z}. \tag{57}$$

Following [4], we put the matrix M in $\mathrm{M}_4(\boldsymbol{Z})$:

$$M := \begin{pmatrix} 2^{k+1} & 2^k & 0 & 0 \\ 2^k & 2^{k+1} & 2^k & 0 \\ 0 & 2^k & 2a & 1 \\ 0 & 0 & 1 & 2b \end{pmatrix},$$

where $a = (2^k - (-1)^k)/3$, $b = (-1)^{k-1}$. The determinant of M is 2^{2k}. We write M also for the $\boldsymbol{Z}$-lattice determined by the matrix M. Then by direct computation, we see that the discriminant form of M is $v_+^{(2)}(2^k)$. Let $F(x) \in \boldsymbol{R}[x]$ be the characteristic polynomial of M: $F(x) = \det(xI - M)$. Then $F(0) = \det M = 2^{2k} > 0$ and $F(2^{k+1}) < 0$. If $k \neq 1$, $F(2b) < 0$. We split the argument into three cases.

CASE 1 $k = 1$. By trivial calculation, $F(0) = 4 > 0$, $F(1) = -12 < 0$, $F(3) = 4 > 0$, $F(4) = -12 < 0$, $F(7) = 60 > 0$. Hence the signature of M is $(4, 0)$. In particular $\operatorname{sgn} v_+^{(2)}(2^k) \equiv 4 \pmod 8$.

CASE 2 k is an odd integer not equals to 1. In this case, $0 < 2b < 2a < 2^{k+1}$, and $F(2a) > 0$. Hence the signature of M is $(4, 0)$, i.e., $\operatorname{sgn} v_+^{(2)}(2^k) \equiv 4 \equiv 4k \pmod 8$.

CASE 3 k is an even integer. In this case, $2b < 0 < 2^{k+1}$. Hence the signature of M is $(2, 2)$. Thus $\operatorname{sgn} v_+^{(2)}(2^k) \equiv 0 \equiv 4k \pmod 8$.

We conclude that the formula (57) holds in all cases.

References

[1] M. Eichler, "Quadratic formen und orthogonale gruppen," Springer-Verlag, Berlin, 1952; Japanese transl. by T. Hiramatsu and Y. Mimura, Springer-Verlag, Tokyo, 1992.

[2] V. V. Nikulin, *Integral symmetric bilinear forms and some of their applications*, Math. USSR Izvestija 14 (1980), No. 1, 103–167.

[3] J. -P. Serre, "Cours d'arithmétique," Presses. Univ. France, Paris, 1970; Japanese transl. by K. Iyanaga, Iwanami shoten, 1970.

[4] C. T. C. Wall, *Quadratic forms on finite groups, and related topics*, Topology 2 (1963), 281–298.