TAMKANG JOURNAL OF MATHEMATICS
Volume 43, Number 1, 11-19, Spring 2012
doi:10.5556/j.tkjm.43.2012.11-19

Available online at http://journals.math.tku.edu.tw/

WEIGHTED QUADRATIC PARTITIONS MODULO P^m A NEW FORMULA AND A NEW DEMONSTRATION

ALI H. HAKAMI

Abstract. Let $Q(\mathbf{x}) = Q(x_1, x_2, \ldots, x_n)$ be a quadratic form over $\mathbb{Z}$, p be an odd prime. Let $V = V_Q = V_{p^m}$ denote the set of zeros of $Q(\mathbf{x})$ in $\mathbb{Z}_{p^m}$ and $|V|$ denotes the cardinality of V. Set $\phi(V_{p^m}, \mathbf{y}) = \sum_{\mathbf{x}\in V} e_{p^m}(\mathbf{x}\cdot\mathbf{y})$ for $\mathbf{y} \neq \mathbf{0}$ and $\phi(V_{p^m}, \mathbf{y}) = \left|V_{p^m}\right| - p^{m(n-1)}$ for $\mathbf{y} = \mathbf{0}$. In this paper, we shall give a formula for the calculation of the function $\phi(V, \mathbf{y})$.

1. Introduction

Let $Q(\mathbf{x}) = Q(x_1, x_2, \ldots, x_n) = \sum_{1\leqslant i\leqslant j\leqslant n} a_{ij} x_i x_j$ be a quadratic form with integer coefficients and p be an odd prime. Suppose that n is even and $\det A_Q \not\equiv 0 \pmod p$, where A_Q is $n \times n$ defining matrix for $Q(\mathbf{x})$. Let $V_{p^m} = V_{p^m}(Q)$ denote the set of zeros of Q in $\mathbb{Z}^n_{p^m}$. Let

$$\Delta_{p^m}(Q) = \begin{cases} \left((-1)^{n/2} \det A_Q/p\right) & \text{if } p \nmid \det A_Q, \\ 0 & \text{if } p \mid \det A_Q, \end{cases}$$

where $(./p)$ denotes the Legendre-Jacobi symbol and let $Q^*(\mathbf{x})$ be the inverse of the matrix representing $Q(\mathbf{x})$, $(\bmod\, p^m)$. For $\mathbf{y} \in \mathbb{Z}^n_{p^m}$ set

$$\phi(V_{p^m}, \mathbf{y}) = \begin{cases} \sum_{\mathbf{x}\in V} e_{p^m}(\mathbf{x}\cdot\mathbf{y}) & \text{for } \mathbf{y} \neq \mathbf{0}, \\ \left|V_{p^m}\right| - p^{m(n-1)} & \text{for } \mathbf{y} = \mathbf{0}, \end{cases}$$

where $e_{p^m}(x) = e^{2\pi i x/p^m}$.

The purpose of this paper is to give an simpler formula for the calculation of the function $\phi(V, \mathbf{y})$. We shall first calculate the Gauss sum

$$S = S(f, p^m) = \sum_{x=1}^{p^m} e_{p^m}\left(f(x)\right), \tag{1}$$

for $f(x) = \lambda a x^2 + xy$, $(\lambda, a, y \in \mathbb{Z})$ and then we apply this sum to calculate the function $\phi(V, \mathbf{y})$. The final result is stated in the following theorem.

2010 *Mathematics Subject Classification*. 11D09, 11L03, 11L05.
Key words and phrases. Quadratic forms, weighted quadratic partitions.

Theorem 1. *Let n be an even positive integer. For $\mathbf{y}\in\mathbb{Z}^n$, put $\mathbf{y}'=p^{-j}\mathbf{y}$ in case $p\,|\,\mathbf{y}$, (i.e., $p\,|\,y_i$ for all i). Then*

$$\phi(V,\mathbf{y})=p^{(mn/2)-m}\sum_{\substack{j=0\\ p^j|y_i \ for\ all\ i}}^{m-1}\delta_j p^{jn/2}\omega_j(\mathbf{y}'),$$

where

$$\delta_j=\begin{cases}1 & if\ m-j\ is\ even,\\ \Delta & if\ m-j\ is\ odd,\end{cases} \tag{2}$$

and

$$\omega_j(\mathbf{y}')=\begin{cases}p^{m-j}-p^{m-j-1}, & p^{m-j}\,|\,Q^*(\mathbf{y}'),\\ -p^{m-j-1}, & p^{m-j-1}\,\|\,Q^*(\mathbf{y}'),\\ 0, & p^{m-j-1}\nmid Q^*(\mathbf{y}').\end{cases} \tag{3}$$

Theorem 1 is given, in other forms in Carlitz papers [1] for $m=1$ and in [2] for $m=$ any positive integer. Also his proof needs some work. We shall devote the rest of §3 to give the proof in complete detail.

2. Preliminaries

In order to proceed from congruences $(\bmod\, p)$ to congruences $(\bmod\, p^m)$, we need to generalize results for exponential sums. Let $\mathbb{Z}_{p^m}=\mathbb{Z}/(p^m)$. Then we have the basic orthogonality relationship that for any $\mathbf{y}\in\mathbb{Z}^n_{p^m}$,

$$\sum_{\mathbf{x}\in\mathbb{Z}^n_{p^m}} e_{p^m}(\mathbf{x}\cdot\mathbf{y})=\begin{cases}p^{mn} & if\ \ \mathbf{y}=\mathbf{0},\\ 0 & if\ \ \mathbf{y}\neq\mathbf{0}.\end{cases} \tag{4}$$

Let $G(p^m)$ denote the multiplicative group of units modulo p^m. Then

Lemma 2. [[**4**], **Lemma 1.5**.] *Let $\lambda,\ a\in\mathbb{Z}$. For any odd prime p and any positive integer m,*

$$\sum_{\lambda\in G(p^m)} e_{p^m}(\lambda a)=\begin{cases}p^m-p^{m-1} & if\ \ p^m\,|\,a,\\ -p^{m-1} & if\ \ p^{m-1}\,\|\,a,\\ 0 & if\ \ p^{m-1}\nmid a.\end{cases}$$

Let g be a polynomial with integer coefficients and let

$$S(g,p^m)=\sum_{x=1}^{p^m} e_{p^m}\left(g(x)\right),$$

where p^m is a prime power with $m \geqslant 2$. Next lemma evaluates and estimates the pure exponential sum $S(g, p^m)$. But to state the statement of this lemma, let $\mathrm{ord}_p(x)$ denote the normal exponent valuation on the p-adic field. In particular, for $x \neq 0 \in \mathbb{Z}$, $p^{\mathrm{ord}_p(x)} \| x$. For convenience, we set $\mathrm{ord}_p(0) = \infty$. For any nonzero polynomial $g = g(X) = a_0 + a_1 X + \cdots + a_d X^d \in \mathbb{Z}[X]$ we define

$$\mathrm{ord}_p(g) := \min_{0 \leqslant i \leqslant d} \{\mathrm{ord}_p(a_i)\}.$$

For any polynomial g over $\mathbb{Z}$ we define

$$t = t(g) := \mathrm{ord}_p\left(g'(X)\right),$$

where $g' = g'(X)$ denotes the derivative of $g(X)$. Also we define the set of critical points associated with the sum $S(g, p^m)$ to be the set

$$\mathscr{A} = \mathscr{A}(g, p) := \{\alpha_1, \ldots, \alpha_D\},$$

of zeros of the congruence

$$p^{-t} g'(x) \equiv 0 \pmod p, \tag{5}$$

where $t = \mathrm{ord}_p(g')$. For any $\alpha \in \mathscr{A}$ let $\nu = \nu_\alpha$ denote the multiplicity of α as a zero of the congruence (5).

Write

$$S(g, p^m) = \sum_{\alpha=0}^{p-1} S_\alpha,$$

where for any integer α,

$$S_\alpha = S_\alpha(g, p^m) := \sum_{\substack{x=1 \\ x \equiv \alpha (\bmod p)}}^{p^m} e_{p^m}(g(x)).$$

Lemma 3. [[3], **Theorem2.1**] *Let p be an odd prime and g be a non-constant polynomial defined over $\mathbb{Z}$. If $m \geqslant t+2$ then for any integer α we have:*

(i) If $\alpha \notin \mathscr{A}$ then $S_\alpha(g, p^m) = 0$.

(ii) If α is a critical point of multiplicity ν then

$$\left|S_\alpha(g, p^m)\right| \leqslant \nu p^{t/(\nu+1)} p^{(m(1-1/(\nu+1)).} \tag{6}$$

(iii) If α is a critical point of multiplicity one then

$$S_\alpha(g, p^m) = \begin{cases} e_{p^m}\left(g(\alpha^*)\right) p^{(m+t)/2} & if\ m-t\ is\ even, \\ \chi(A_\alpha)\, e_{p^m}\left(g(\alpha^*)\right) G_p p^{(m+t-1)/2} & if\ m-t\ is\ odd, \end{cases}$$

where α^* *is the unique lifting of* α^* *to a solution of the congruence* $p^{-t}g'(x) \equiv 0 \pmod{p^{[(m-t+1)/2]}}$, *and* $A_\alpha \equiv 2p^{-t}g''(\alpha^*) \pmod p$*. In particular, we have equality in (6). Here* G_p *is the classical Gauss sum,*

$$G_p := \sum_{x=1}^{p} e_p(x^2) = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \pmod 4, \\ i\sqrt{p} & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

and χ *is the quadratic character* mod p.

3. Determination of $\phi(V, \mathbf{y})$ modulo p^m

We start this section by calculating the sum $S(f, p^m)$. The following lemma allows us to find the evaluation of $\phi(V, \mathbf{y})$. A special case of this lemma (when $m = 2$) was proved in [[4], Lemma 2.3].

Lemma 4. *Let* p *be an odd prime with* $p \nmid a$ *and* λ, $a \in \mathbb{Z}$*. Let the sum* S *as in (1). Let* $j \in \{0, 1, 2, \ldots, m-1\}$*. Then*

$$S = \begin{cases} e_{p^{m-j}}(-\bar{4}\bar{a}\bar{\lambda}' y'^2) p^{(m+j)/2} & if\ p^j \parallel \lambda,\ p^j \mid y \text{ and } m-j \text{ is even}, \\ \chi\left(4a\lambda'\right) e_{p^{m-j}}\left(-\bar{4}\bar{a}\bar{\lambda}' y'^2\right) G_p p^{(m+j-1)/2} & if\ p^j \parallel \lambda,\ p^j \mid y \text{ and } m-j \text{ is odd}, \\ 0 & if\ p^j \parallel \lambda,\ but\ p^j \nmid y, \end{cases}$$

where χ *is the Legendre Symbol*, $\lambda' = \lambda p^{-j}$, $y' = y p^{-j}$ *and* $\bar{\lambda}$, $\bar{\lambda}'$, $\bar{a}$ *are inverses* mod p^m.

Proof. We shall require applying Lemma 2. Assume that $p \nmid a$. Then the critical point congruence is

$$p^{-t} f'(x) \equiv 0 \pmod p,$$

or equivalently,

$$p^{-t}(\lambda a 2x + y) \equiv 0 \pmod p, \tag{7}$$

where $t = \mathrm{ord}_p(f')$. Now we have to treat two cases:

Case (i): Assume that $p^j \parallel \lambda$ and $p^j \mid y$, with $j \in \{0, 1, 2, \ldots, m-1\}$. Then $t = j$ because $p^t \parallel (2a\lambda, y)$. Thus (7) is equivalent to

$$2a\frac{\lambda}{p^j}\, x \equiv -\frac{y}{p^j} \pmod p. \tag{8}$$

Put $\lambda' = \lambda / p^j$ and $y' = y / p^j$, then (8) becomes

$$2a\lambda'\, x \equiv -y' \pmod p,$$

or equivalently, there is a unique critical point α given by

$$\alpha = x \equiv -\overline{2a\lambda'}y' \pmod p.$$

Thus if $m-j$ is even,

$$S = S_\alpha = e_{p^m}\left(f(\alpha^*)\right)p^{(m+t)/2} = e_{p^m}\left(\lambda a {\alpha^*}^2 + y\alpha^*\right)p^{(m+j)/2},$$

where α^* is the unique lifting of α, to a solution of (7) $\bmod p^{(m-j+1)/2}$. We can take $\alpha^* \equiv -\bar{2}\,\bar{a}\,\bar{\lambda}'\,y' \pmod{p^m}$ where $\bar{a}$, $\bar{\lambda}$ are inverses $\bmod p^m$. Then

$$\begin{aligned} f(\alpha^*) = \lambda a\alpha^{*2} + y\alpha^* &\equiv p^j\lambda' a\overline{\lambda'}^2\bar{4}\bar{a}^2y'^2 - p^jy'^2\bar{\lambda}'\overline{2a} \pmod{p^m}\\ &\equiv p^jy'^2(\bar{4}\bar{a}\overline{\lambda'} - \bar{2}\bar{a}\overline{\lambda'}) \pmod{p^m}\\ &\equiv -\bar{4}\bar{a}\bar{\lambda}'y'^2p \pmod{p^m}\end{aligned}$$

and so $S_\alpha = e_{p^{m-j}}(-\bar{4}\bar{a}\bar{\lambda}'y'^2)p^{(m+j)/2}$.

If $m-j$ is odd, then

$$A_\alpha \equiv 2p^{-t}f''(\alpha^*) \equiv 2p^{-j}2a\lambda \equiv 4a\lambda' \pmod p.$$

Thus

$$\begin{aligned} S = S_\alpha &= \chi(A_\alpha)\,e_{p^m}(\lambda a\alpha^{*2} + y\alpha^*)G_p p^{(m+j-1)/2}\\ &= \chi(4a\lambda')\,e_{p^{m-j}}(-\bar{4}\bar{a}\bar{\lambda}'y'^2)G_p p^{(m+j-1)/2}.\end{aligned}$$

Case (ii): Suppose that $p^j \,\|\, \lambda$ but $p^j \nmid y$, with $j \in \{1,2,\dots,m-1\}$; say $p^k \,\|\, y$ with $k<j$. Then we see that $t=k$. By (7), the critical point congruence is

$$p^t(2a\lambda x) \equiv -yp^{-t} \pmod p,$$

or equivalently,

$$0 \equiv -yp^k \pmod p,$$

which has no solution. Consequently $S=0$, and this completes the proof of Lemma 3. □

Now we shall evaluate $\phi(V,\mathbf{y})$ for the case of a diagonal quadratic form.

Suppose that $(\mathbf{x}) = \sum_{i=1}^n a_ix_i^2$; with $p\nmid a_i,\ 1\leqslant i\leqslant n$. We remark that if $\mathbf{y}\neq\mathbf{0}$, then by the orthogonality property of exponential sums,

$$\begin{aligned}\sum_{\mathbf{x}\in\mathbf{V}} e_{p^m}(\mathbf{x}\cdot\mathbf{y}) &= \sum_{\mathbf{x}\in\mathbb{Z}_{p^m}^n} p^{-m}\left(\sum_{\lambda=0}^{p^m-1} e_{p^m}(\lambda Q(\mathbf{x}))\right)e_{p^m}(\mathbf{x}\cdot\mathbf{y})\\ &= p^{-m}\sum_\lambda\sum_{\mathbf{x}} e_{p^m}(\lambda Q(\mathbf{x}) + \mathbf{x}\cdot\mathbf{y})\end{aligned}$$

$$= \underbrace{p^{-m}\sum_{\mathbf{x}} e_{p^m}(\mathbf{x}\cdot\mathbf{y})}_{S_1} + \underbrace{p^{-m}\sum_{\lambda\neq 0}\sum_{\mathbf{x}} e_{p^m}(\lambda Q(\mathbf{x})+\mathbf{x}\cdot\mathbf{y})}_{S_2}.$$

Now, if $\mathbf{y}=\mathbf{0}$, this implies that

$$|V| = p^{m(n-1)} + S_2 \quad\Rightarrow\quad S_2 = |V| - p^{m(n-1)} = \phi(V,\mathbf{0}).$$

Next suppose that $\mathbf{y}\neq\mathbf{0}$. Then, by (4), as some $y_i\neq 0$,

$$S_1 = p^{-m}\sum_{\mathbf{x}} e_{p^m}(\mathbf{x}\cdot\mathbf{y}) = p^{-m}\prod_{i=1}^{n}\sum_{x_i}^{p^m} e_{p^m}(x_i y_i) = 0,$$

while

$$\begin{aligned} S_2 &= p^{-m}\sum_{\lambda\neq 0}\sum_{\mathbf{x}} e_{p^m}(\lambda Q(\mathbf{x})+\mathbf{x}\cdot\mathbf{y}) \\ &= p^{-m}\sum_{\lambda\neq 0}\underbrace{\sum_{\mathbf{x}} e_{p^m}\left(\lambda(a_1x_1^2+a_2x_2^2+\cdots+a_nx_n^2)+x_1y_1+x_2y_2+\cdots+x_ny_n\right)}_{S_\lambda}. \end{aligned} \tag{9}$$

Hence we have $S_2=\phi(V,\mathbf{y})$ for all $\mathbf{y}$. From now on we shall use $\phi(V,\mathbf{y})$ to mean S_2 and vice versa. The inside sum S_λ in (9) may be rewritten

$$\begin{aligned} S_\lambda &= \sum_{\mathbf{x}} e_{p^m}\left([\lambda a_1x_1^2+x_1y_1]+\cdots+[\lambda a_nx_n^2+y_nx_n]\right) \\ &= \sum_{x_1} e_{p^m}(\lambda a_1x_1^2+y_1x_1)\cdots\sum_{x_n} e_{p^m}(\lambda a_nx_n^2+y_nx_n) \\ &= \prod_{i=1}^{n}\underbrace{\sum_{x_i=1}^{p^m} e_{p^m}(\lambda a_ix_1^2+x_iy_i)}_{\text{Gauss sum}}. \end{aligned} \tag{10}$$

As a consequence of Lemma 3, we have the following Lemma.

Lemma 5. *Suppose n is even. Let S_λ as in (10). Let $p^j\,\|\,\lambda$, $0\leqslant j\leqslant m-1$. Assume $p\nmid a_1\cdot a_2\cdot\cdots\cdot a_n$. Then*

$$S_\lambda = \begin{cases} \delta_j p^{(m+j)n/2} e_{p^{m-j}}(-\overline{4\lambda'}Q^*(\mathbf{y}')) & if\ p^j\,|\,y_i\ for\ all\ i, \\ 0 & if\ p^j\nmid y_i, for\ some\ i, \end{cases} \tag{11}$$

where $\lambda' = p^{-j}\lambda$, $y' = p^{-j}y$ *and*

$$\delta_j = \begin{cases} 1 & if\ m-j\ is\ even, \\ \Delta & if\ m-j\ is\ odd, \end{cases}$$

with $\Delta = \chi\left((-1)^{n/2}\right)\chi(a_1\cdots a_n)$.

Proof. First let us suppose that $p^j \| \lambda$ and that $p^j \,|\, y_i$ for all i. Put $\lambda' = p^{-j}\lambda$ and $y_i' = p^{-j}y_i$. Then by Lemma 3, if $m-j$ is even,

$$\begin{aligned} S_\lambda &= e_{p^{m-j}}(-\bar{4}\overline{a_1}\bar{\lambda}' y_1'^2)p^{(m+j)/2}\cdots e_{p^{m-j}}(-\bar{4}\overline{a_n}\bar{\lambda}' y_n'^2)p^{(m+j)/2} \\ &= p^{(m+j)n/2}e_{p^{m-j}}\left((-\bar{4})\overline{a_1}\,\bar{\lambda}' y_1'^2 + (-\bar{4})\overline{a_2}\bar{\lambda}' y_2'^2 + \cdots + (-\bar{4})\overline{a_n}\,\bar{\lambda}' y_n'^2\right) \\ &= p^{(m+j)n/2}e_{p^{m-j}}\underbrace{\left(\left((-\bar{4})\,\bar{\lambda}'\right)\left(\overline{a_1}y_1'^2 + \overline{a_2}y_2'^2 + \cdots + \overline{a_n}\,y_n'^2\right)\right)}_{-\bar{4}\bar{\lambda}Q^*(y_1,\dots,y_n)=\overline{-4\lambda}Q^*(\mathbf{y}),} \\ &= p^{(m+j)n/2}e_{p^{m-j}}\left(-\bar{4}\bar{\lambda}'Q^*(\mathbf{y}')\right), \end{aligned}$$

where $Q^*(\mathbf{y})$, as defined earlier, is the quadratic form associated with the inverse of the matrix for $Q \bmod p^m$. If $m-j$ is odd, then again by Lemma 3,

$$\begin{aligned} S_\lambda &= \chi(4a_1\lambda')\,e_{p^{m-j}}(-\bar{4}\bar{a}_1\bar{\lambda}' y_1'^2)G_p p^{(m+j-1)/2}\cdot\cdots \\ &\qquad\qquad \cdot\chi(4a_1\lambda')\,e_{p^{m-j}}(-\bar{4}\bar{a}_n\bar{\lambda}' y_n'^2)G_p p^{(m+j-1)/2} \\ &= p^{n(m+j-1)/2}G_{p^n}\,\chi(4\lambda' a_1\cdots 4\lambda' a_n)\,e_{p^{m-j}}\left(\overline{(-4)}\,\bar{\lambda}'Q^*(y_1'^2 + y_2'^2 + \cdots + y_n'^2)\right) \\ &= p^{n(m+j-1)/2}p^{n/2}\overbrace{\chi((-1)^{n/2})\,\underbrace{\chi(a_1\cdots a_n)}_{n\text{ is even}}}^{\Delta}\,e_{p^{m-j}}\left(\overline{(-4)}\,\bar{\lambda}'\,Q^*(\mathbf{y}')\right) \\ &= p^{n(m+j)/2}\Delta e_{p^{m-j}}\left(\overline{(-4)}\,\bar{\lambda}'\,Q^*(\mathbf{y}')\right). \end{aligned}$$

Next suppose that $p^j \| \lambda$ but $p^j \nmid y_i$ for some i. Then it is easily seen that (by Lemma 3) $S_\lambda = 0$. Thus the proof of Lemma 4 is complete. □

By our discussion which will come later in §4, Lemma 4 can be generalized to an arbitrary nonsingular quadratic form $(\bmod\ p^m)$ as follows.

Lemma 6. *Let p be an odd prime, n be even and $Q(\mathbf{x})$ any quadratic form. Let $p^j \| \lambda$, $0 \leqslant j \leqslant m-1$. Assume* $\det A_Q \not\equiv 0 (\bmod\ p)$, *where A_Q is the $n\times n$ defining matrix for $Q(\mathbf{x})$. Then*

$$S_\lambda = \begin{cases} \delta_j p^{(m+j)n/2}e_{p^{m-j}}(-\overline{4\lambda'}Q^*(\mathbf{y}')) & if\ p^j\,|\,y_i,\ for\ all\ i\,, \\ 0 & if\ p^j \nmid y_i,\ for\ some\ i, \end{cases}$$

where $\lambda' = p^{-j}\lambda$, $y' = p^{-j}y$ *and* δ_j *as given in (2).*

We are now ready to prove Theorem 1

Proof of Theorem 1. Recall that $\phi(V,\mathbf{y}) = p^{-m}\sum_{\lambda\neq 0} S_\lambda = S_2$. Fix $\mathbf{y} = (y_1,\ldots,y_n)$. Put $\mathbf{y}' = p^{-j}\mathbf{y}$, $\lambda' = p^{-j}\lambda$. Then according to Lemma 5,

$$\begin{aligned}
\sum_{\lambda=1}^{p^m-1} S_\lambda &= \sum_{\substack{j=0\\ p^j|y_i,\text{ for all } i}}^{m-1} \sum_{\substack{\lambda\\ p^j\|\lambda}} \delta_j p^{(m+j)n/2} e_{p^{m-j}}\left(-\bar{4}\bar{\lambda}' Q^*(\mathbf{y}')\right)\\
&= \sum_{\substack{j=0\\ p^j|y_i,\text{ for all } i}}^{m-1} \delta_j p^{(m+j)n/2} \sum_{\substack{\lambda'=1\\ p\nmid\lambda'}}^{p^{m-j}} e_{p^{m-j}}\left(-\bar{4}\bar{\lambda}' Q^*(\mathbf{y}')\right)\\
&= \sum_{\substack{j=0\\ p^j|y_i,\text{ for all } i}}^{m-1} \delta_j p^{(m+j)n/2}\,\omega_j(\mathbf{y}'),
\end{aligned}$$

where we have used Lemma 1 applied to the second sum in the second step above. Hence, it follows that

$$\phi(V,\mathbf{y}) = p^{-m} \sum_{\substack{j=0\\ p^j|y_i,\text{ for all } i}}^{m-1} \delta_j p^{(m+j)n/2}\,\omega_j(\mathbf{y}') = p^{(mn/2)-m} \sum_{\substack{j=0\\ p^j|y_i\ \text{for all } i}}^{m-1} \delta_j p^{jn/2}\omega_j(\mathbf{y}').$$

This completes the proof of Theorem 1. □

4. Remark

In the last section we calculated $\phi(V,\mathbf{y})$ for the case of diagonal quadratic forms. Suppose now that $Q(\mathbf{x})$ is any quadratic form. Let V_{p^m} be the set of solution of the quadratic congruence $Q(\mathbf{x}) \equiv 0 \,(\mathrm{mod}\, p^m)$. Let $\mathbf{x} = T(\mathbf{u})$ where T is a transformation that diagonalizes Q, so that $Q(T(\mathbf{u})) = Q_1(\mathbf{u})$, a diagonal quadratic form. Let V'_{p^m} be the set of solution of the quadratic congruence $Q_1(\mathbf{u}) \equiv 0 (\mathrm{mod}\, p^m)$. Set $T^t(\mathbf{y}) = \mathbf{v}$. We first show that $\phi(V_{p^m},\mathbf{y}) = \phi(V'_{p^m},\mathbf{v})$. Note that, since T is a nonsingular transformation $\mathrm{mod}\, p$, $\mathbf{y} \equiv \mathbf{0} \,(\mathrm{mod}\, p)$ is equivalent to $\mathbf{v} \equiv \mathbf{0}\,(\mathrm{mod}\, p)$. If $\mathbf{y} \equiv \mathbf{0}\ (\mathrm{mod}\, p)$, then

$$\phi(V_{p^m},\mathbf{y}) = \left|V_{p^m}\right| - p^{2(n-1)} = \left|V'_{p^m}\right| - p^{2(n-1)} = \varphi(V'_{p^m},\mathbf{v}).$$

For $\mathbf{y} \not\equiv \mathbf{0}\,(\mathrm{mod}\, p)$, we have

$$\begin{aligned}
\phi(V_{p^m},\mathbf{y}) &= \sum_{\mathbf{x}\in V_{p^m}} e_{p^m}(\mathbf{x}\cdot\mathbf{y})\\
&= \sum_{Q(\mathbf{x})\equiv 0(\bmod p^m)} e_{p^m}(\mathbf{x}\cdot\mathbf{y})
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{Q(T(\mathbf{u}))\equiv 0(\bmod p^m)} e_{p^m}(T(\mathbf{u})\cdot \mathbf{y}) \\
&= \sum_{Q_1(\mathbf{u})\equiv 0(\bmod p^m)} e_{p^m}(\mathbf{u}\cdot T^t(\mathbf{y})) \\
&= \sum_{\mathbf{u}\in V'_{p^m}} e_{p^m}(\mathbf{u}\cdot T^t(\mathbf{y})) \\
&= \phi(V'_{p^m}, T^t(\mathbf{y})) \\
&= \phi(V'_{p^m}, \mathbf{v}).
\end{aligned}
$$

Say $Q(\mathbf{x}) = \mathbf{x}^t A_Q \mathbf{x}$, where A_Q is the associated matrix for Q. Then

$$
Q_1(\mathbf{u}) = Q(T(\mathbf{u})) = (T(\mathbf{u}))^t A_Q (T(\mathbf{u})) = \mathbf{u}^t \underbrace{T^t A_Q T}_{A_{Q_1}} \mathbf{u}
$$

And

$$
Q_1^*(\mathbf{v}) = Q_1^*\left(T^t(\mathbf{y})\right) = \left(T^t\mathbf{y}\right)^t \left[T^{-1}A_Q^{-1}(T^t)^{-1}\right] T^t(\mathbf{y}) = \mathbf{y}^{\mathbf{t}} A_Q^{-1}\mathbf{y} = Q_1^*(\mathbf{y}).
$$

Thus by our result for diagonal forms we have for the original quadratic form that

$$
\phi(V,\mathbf{y}) = p^{(mn/2)-m} \sum_{\substack{j=0 \\ p^j | y_i \text{ for all } i}}^{m-1} \delta_j p^{jn/2} \omega_j(\mathbf{y}'),
$$

where δ_j and ω_j as defined in (2) and (3).

Acknowledgement

The author would like to thank the anonymous referee for his productive and useful comments and suggestions.

References

[1] L. Carlitz, *Weighted quadratic partitions over a finite field*, Cand. J. Math., **5** (1953), 317–323.

[2] ——, *Weighted quadratic partitions* $(mod\ p^r)$, Math Zeitschr. Bd., **59**(1953), 40–46.

[3] T. Cochrane and Z. Zheng, *Pure and mixed exponential sums*, Acta Arithmetica, XCI.3. (1999), 249–278.

[4] A. Hakami, Small zeros of quadratic congruences to a prime power modulus. PhD thesis, Kansas State University, 2009.

Department of Mathematics, King Khalid University, P.O.Box 9004, Abha, Postal Code: 61431, Saudi Arabia.

E-mail: aalhakami@kku.edu.sa