Alabama Journal of Mathematics
40 (2016)
ISSN 2373-0404

Counting lattice points of quadratic forms over the ring $\mathbb{Z}_{p^3}$

Ali H. Hakami
Department of Mathematics
Science Faculty of Jazan University

Let $Q(\mathbf{x}) = Q(x_1, x_2, \ldots, x_n)$ be a quadratic form in n-variables with integer coefficients. We obtain bounds on the lattice points over the ring $\mathbb{Z}^n_{p^3}$ to the congruence $Q(\mathbf{x}) \equiv 0 \pmod{p^3}$ in a general rectangular box. We use Fourier series and exponential sums to obtain our results.

Introduction

Let $Q(\mathbf{x}) = Q(x_1, x_2, ..., x_n) = \sum_{1\leqslant i\leqslant j\leqslant n} a_{ij}x_ix_j$, be a nonsingular quadratic form with integer coefficients in n-variables. Let $V_{p^3,\mathbb{Z}} = V_{p^3,\mathbb{Z}}(Q)$ be the set of integer solutions of the equation defined by

$$Q(\mathbf{x}) \equiv 0 \pmod{p^3}, \tag{1}$$

(in $\mathbb{Z}^n_{p^3}$) and and let $\mathcal{B}$ be a box defined by

$$\mathcal{B} = \{\mathbf{x} \in \mathbb{Z}^n \mid a_i \leqslant x_i < a_i + m_i,\ 1 \leqslant i \leqslant n\}, \tag{2}$$

where $a_i, m_i \in \mathbb{Z}$, and $0 \leqslant m_i \leqslant p^3$ for $1 \leqslant i \leqslant n$. Let $|\mathcal{B}|$ denote the cardinality of the box $\mathcal{B}$. We call the box a cube of size m if $m_i = m$ for all i. Suppose that n is even and and A_Q is the $n\times n$ defining matrix for $Q(\mathbf{x})$. Let

$$\Delta = \Delta_p(Q) = \left(\frac{(-1)^{\frac{n}{2}} \det A_Q}{p}\right),$$

where $(./p)$ denotes the Legendre-Jacobi symbol. In this paper we shall use Fourier series and exponential sums to find points in V with the variables restricted to the box $\mathcal{B}$ of the type (2), so that $V \cap \mathcal{B}$ is non empty and determine the cardinality $|V \cap \mathcal{B}|$ of $V \cap \mathcal{B}$. We have the following main result:

Theorem 1. *Let p be an odd prime, n positive integer and Q is nonsingular quadratic form. Let $V = V_{p^3}(Q)$ be the set of integer solutions of the congruence (1) in $\mathbb{Z}^n_{p^3}$ and $\mathcal{B}$ be a box as given in (2) centered at the origin with all $m_i \leqslant p^3$. If* $\Delta = \pm1$. *Then*

$$\left|\mathcal{B} \cap V_{p^3}\right| \leqslant \begin{cases} \upsilon_n\left(\frac{|\mathcal{B}|}{p^3} + p^{(3n/2)-1}\right) & if\ \ \Delta = -1, \\ \upsilon_n\left(\frac{|\mathcal{B}|}{p^3} + p^{3n/2}\right) & if\ \ \Delta = +1, \end{cases} \tag{3}$$

where the brackets $|\ .\ |$ are used to denote the cardinality of the set inside the brackets, and

$$\upsilon_n = \begin{cases} 2^n\left(1 + 2^n + \frac{2^{(n/2)+1}}{p}\right), & \Delta = -1, \\ 2^n\left(1 + 2^n + 2^{(n/2)+1}\right), & \Delta = +1. \end{cases} \tag{4}$$

Corresponding Author Email: aalhakami@jazanu.edu.sa

Historically, there are a lot of known results on the solutions of quadratic forms (mod p), (mod p^2) and (mod p^m) (see for example, Cochrane (1984, 1989, 1990, 1991); Cochrane and Hakami (2012); Hakami (2009, 2011a, 2011b, 2011c, 2012, 2014a, 2014b, 2015); Heath-Brown (1985, 1991); Schinzel, Schlickewei, and Schmidt (1980); Wang (1989, 1990, 1993)).

We shall devote the last section to give the proof of Theorem 1. If V is the set of zeros of a nonsingular quadratic form $Q(\mathbf{x})$, then one can show that

$$|V \cap \mathcal{B}| = \frac{|\mathcal{B}|}{p} + O\left(p^{n/2} (\log p)^{3n}\right), \tag{5}$$

for any box $\mathcal{B}$ (see Cochrane (1984) and Hakami (2009)). It is apparent from (5) that $|V \cap \mathcal{B}|$ is nonempty provided

$$|\mathcal{B}| \gg p^{(n/2)+1} (\log p)^{3n}.$$

For any $\mathbf{x}$, $\mathbf{y}$ in $\mathbb{Z}^n_{p^3}$, we let $\mathbf{x}\cdot\mathbf{y}$ denote the ordinary dot product, $\mathbf{x}\cdot\mathbf{y} = \sum_{i=1}^n x_iy_i$. For any $x \in \mathbb{Z}_{p^3}$, let $e_{p^3}(x) = e^{2\pi ix/p^3}$. We use the abbreviation $\sum_{\mathbf{x}} = \sum_{\mathbf{x}\in\mathbb{Z}^n_{p^3}}$ for complete sums. The key ingredient in obtaining the identity in (5) is a uniform upper bound on the function

$$\phi(V, \mathbf{y}) = \begin{cases} \sum_{\mathbf{x}\in V} e_{p^3}(\mathbf{x}\cdot\mathbf{y}), & \mathbf{y} \neq \mathbf{0}, \\ |V| - p^{3(n-1)}, & \mathbf{y} = \mathbf{0}. \end{cases} \tag{6}$$

In order to show that $\mathcal{B} \cap V$ is nonempty we can proceed as follows. Let $\alpha(\mathbf{x})$ be a complex valued function on $\mathbb{Z}^n_{p^3}$ such that $\alpha(\mathbf{x}) \leqslant 0$ for all $\mathbf{x}$ not in $\mathcal{B}$. If we can show that $\sum_{\mathbf{x}\in V} \alpha(\mathbf{x}) > 0$, then it will follow that $\mathcal{B} \cap V$ is nonempty. Now $\alpha(\mathbf{x})$ has a finite Fourier expansion

$$\alpha(\mathbf{x}) = \sum_{\mathbf{y}} a(\mathbf{y})\, e_{p^3}(\mathbf{y}\cdot\mathbf{x}),$$

where

$$a(\mathbf{y}) = p^{-3n} \sum_{\mathbf{x}} \alpha(\mathbf{x})\, e_{p^3}(-\mathbf{y}\cdot\mathbf{x}),$$

for all $\mathbf{y} \in \mathbb{Z}^n_{p^3}$. Thus

$$\begin{aligned}\sum_{\mathbf{x}\in V}\alpha(\mathbf{x}) &= \sum_{\mathbf{x}\in V}\sum_{\mathbf{y}} a(\mathbf{y})\, e_{p^3}(\mathbf{y}\cdot\mathbf{x}) \\ &= \sum_{\mathbf{y}} a(\mathbf{y}) \sum_{\mathbf{x}\in V} e_{p^3}(\mathbf{y}\cdot\mathbf{x}) \\ &= a(\mathbf{0})\,|V| + \sum_{\mathbf{y}\neq\mathbf{0}} a(\mathbf{y}) \sum_{\mathbf{x}\in V} e_{p^3}(\mathbf{y}\cdot\mathbf{x}).\end{aligned}$$

Since $a(\mathbf{0}) = p^{-3n}\sum_{\mathbf{x}}\alpha(\mathbf{x})$, we obtain

$$\sum_{\mathbf{x}\in V}\alpha(\mathbf{x}) = p^{-3n}\,|V|\sum_{\mathbf{x}}\alpha(\mathbf{x}) + \sum_{\mathbf{y}\neq\mathbf{0}} a(\mathbf{y})\,\phi(V,\mathbf{y}), \tag{7}$$

where $\phi(V,\mathbf{y})$ is defined by (6). A variation of (7) that is sometimes more useful is

$$\sum_{\mathbf{x}\in V}\alpha(\mathbf{x}) = p^{-3}\sum_{\mathbf{x}}\alpha(\mathbf{x}) + \sum_{\mathbf{y}} a(\mathbf{y})\,\phi(V,\mathbf{y}), \tag{8}$$

which is obtained from (7) by noticing that $|V| = \phi(V,\mathbf{0}) + p^{3(n-1)}$, whence

$$\begin{aligned}\sum_{\mathbf{x}\in V}\alpha(\mathbf{x}) &= a(\mathbf{0})[\phi(V,\mathbf{0}) + p^{3(n-1)}] + \sum_{\mathbf{y}\neq\mathbf{0}} a(\mathbf{y})\,\phi(V,\mathbf{y}) \\ &= p^{3n-3}a(\mathbf{0}) + \sum_{\mathbf{y}} a(\mathbf{y})\,\phi(V,\mathbf{y}).\end{aligned}$$

Equations (7) and (8) express the incomplete sum $\sum_{\mathbf{x}\in V}\alpha(\mathbf{x})$ as a fraction of the complete sum $\sum_{\mathbf{x}}\alpha(\mathbf{x})$ plus an error term. In general $|V| \approx p^{3(n-1)}$ so that the fractions in the two equations are about the same. In fact, if V is defined by a nonsingular quadratic form $Q(\mathbf{x})$ then $|V| = p^{3(n-1)} + O(p^n)$ (that is $|\phi(V,\mathbf{0})| \ll p^n$).

To show that $\sum_{\mathbf{x}\in V}\alpha(\mathbf{x})$ is positive, it suffices to show that the error term is smaller in absolute value than the (positive) main term on the right-hand side of (7) or (8). One tries to make an optimal choice of $\alpha(\mathbf{x})$ in order to minimize the error term. Special cases of (7) and (8) have appeared a number of times in the literature for different types of algebraic sets V; see Chalk (1963), Tietäväinen (1967), and Myerson (1991). The first case treated was to let $\alpha(\mathbf{x})$ be the characteristic function $\chi_S(\mathbf{x})$ of a subset S of $\mathbb{Z}^n_{p^3}$, whence (8) gives rise to formulas of the type

$$|V\cap S| = p^{-3}\,|S| + Error.$$

Equation (5) is obtained in this manner. Particular attention has been given to the case where $S = \mathcal{B}$, a box of points in $\mathbb{Z}^n_{p^3}$. Another popular choice for α is let it be a convolution of two characteristic functions, $\alpha = \chi_S * \chi_T$ for $S, T \subseteq \mathbb{Z}^n_{p^3}$. We recall that if $\alpha(\mathbf{x})$, $\beta(\mathbf{x})$ are complex valued functions defined on $\mathbb{Z}^n_{p^3}$, then the convolution of $\alpha(\mathbf{x})$, $\beta(\mathbf{x})$ written $\alpha * \beta(\mathbf{x})$, is defined by

$$\alpha * \beta(\mathbf{x}) = \sum_{\mathbf{u}}\alpha(\mathbf{u})\beta(\mathbf{x}-\mathbf{u}) = \sum_{\mathbf{u}+\mathbf{v}=\mathbf{x}}\alpha(\mathbf{u})\beta(\mathbf{v}),$$

for $\mathbf{x} \in \mathbb{Z}^n_{p^3}$. If we take $\alpha(\mathbf{x}) = \chi_S * \chi_T(\mathbf{x})$ then it is clear from the definition that $\alpha(\mathbf{x})$ is the number of ways of expressing $\mathbf{x}$ as a sum $\mathbf{s}+\mathbf{t}$ with $\mathbf{s}\in S$ and $\mathbf{t}\in T$. Moreover, $(S+T)\cap V$ is nonempty if and only if $\sum_{\mathbf{x}\in V}\alpha(\mathbf{x}) > 0$.

We make use of a number of basic properties of finite Fourier series, which are listed below. They are based on the orthogonality relationship,

$$\sum_{\mathbf{x}\in\mathbb{Z}^n_{p^3}} e_{p^3}(\mathbf{x}\cdot\mathbf{y}) = \begin{cases} p^{3n}, & \mathbf{y}=\mathbf{0}, \\ 0, & \mathbf{y}\neq\mathbf{0}, \end{cases}$$

and they can be routinely checked. By viewing $\mathbb{Z}^n_{p^3}$ as a $\mathbb{Z}$−module, the Gauss sum

$$S_p(Q,\mathbf{y}) = \sum_{\mathbf{x}\in\mathbb{Z}^n_{p^3}} e_{p^3}\,(Q(\mathbf{x}) + \mathbf{y}\cdot\mathbf{x}),$$

is well defined whether we take $\mathbf{y}\in\mathbb{Z}^n$ or $\mathbf{y}\in\mathbb{Z}^n_{p^3}$. Let $\alpha(\mathbf{x})$, $\beta(\mathbf{x})$ be complex valued functions on $\mathbb{Z}^n_{p^3}$ with Fourier expansions

$$\alpha(\mathbf{x}) = \sum_{\mathbf{y}} a(\mathbf{y})\,e_{p^3}(\mathbf{x}\cdot\mathbf{y}),\quad \beta(\mathbf{x}) = \sum_{\mathbf{y}} b(\mathbf{y})\,e_{p^3}(\mathbf{x}\cdot\mathbf{y}).$$

Then

$$\alpha * \beta(\mathbf{x}) = \sum_{\mathbf{y}} p^{3n}a(\mathbf{y})\,b(\mathbf{y})\,e_{p^3}(\mathbf{x}\cdot\mathbf{y}), \tag{9}$$

$$\alpha\beta(\mathbf{x}) = \alpha(\mathbf{x})\beta(\mathbf{x}) = \sum_{\mathbf{y}} (a * b)(\mathbf{y})\,e_{p^3}(\mathbf{x}\cdot\mathbf{y}), \tag{10}$$

$$\sum_{\mathbf{x}}(\alpha*\beta)(\mathbf{x}) = \left(\sum_{\mathbf{x}}\alpha(\mathbf{x})\right)\left(\sum_{\mathbf{x}}\beta(\mathbf{x})\right), \tag{11}$$

$$\sum_{\mathbf{x}}|(\alpha*\beta)(\mathbf{x})| \leqslant \left(\sum_{\mathbf{x}}|\alpha(\mathbf{x})|\right)\left(\sum_{\mathbf{x}}|\beta(\mathbf{x})|\right), \tag{12}$$

$$\sum_{\mathbf{y}}|a(\mathbf{y})|^2 = p^{-3n}\sum_{\mathbf{x}}|\alpha(\mathbf{x})|^2. \tag{13}$$

The last identity is Parseval's equality.

Fundamental Identity

Let $Q(\mathbf{x}) = Q(x_1,...,x_n)$ be a quadratic form with integer coefficients and p be an odd prime. Consider the congruence (1):

$$Q(\mathbf{x}) \equiv 0 \pmod{p^3}.$$

Using identities for the Gauss sum $S = \sum_{x=1}^{p^3} e_{p^3}(ax^2+bx)$, one obtains

Lemma 1. [Hakami (2012), Theorem 1] *Suppose n is even, Q is nonsingular* (mod p) *and $\Delta = \Delta_p(Q)$. 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*

$$\phi(V,\mathbf{y}) = p^{(3n/2)-3}\sum_{\substack{j=0\\ p^j|y_i\ for\,all\,i}}^{2}\delta_j p^{jn/2}\omega_j(\mathbf{y}'),$$

with

$$\delta_j = \begin{cases} 1 & if\ 3-j\ is\ even, \\ \Delta & if\ 3-j\ is\ odd, \end{cases}$$

and

$$\omega_j(\mathbf{y}') = \begin{cases} p^{3-j} - p^{2-j}, & p^{3-j}\,|Q^*(\mathbf{y}'), \\ -p^{2-j}, & p^{2-j}\,\|Q^*(\mathbf{y}'), \\ 0, & p^2 \nmid Q^*(\mathbf{y}'), \end{cases}$$

where Q^* is the quadratic form associated with the inverse of the matrix for Q (mod p).

Back to (8) we saw the identity

$$\sum_{\mathbf{x}\in V} \alpha(\mathbf{x}) = p^{-3} \sum_{\mathbf{x}} \alpha(\mathbf{x}) + \sum_{\mathbf{y}\neq 0} a(\mathbf{y})\,\phi(V,\mathbf{y}).$$

Inserting the value $\phi(V,\mathbf{y})$ in Lemma 1 yields (see Hakami (2011c)),

Lemma 2. *(**The fundamental identity**) For any complex valued $\alpha(\mathbf{x})$ on $\mathbb{Z}^n_{p^3}$, if $\Delta = +1$, then*

$$\begin{aligned}\sum_{\mathbf{x}\in V_{p^3}} \alpha(\mathbf{x}) &= p^{-3} \sum_{\mathbf{x}} \alpha(\mathbf{x}) + p^{3n/2} \sum_{\substack{y_i=1 \\ p^3|Q^*(\mathbf{y})}}^{p^3} a(\mathbf{y}) \\ &+ p^{2n-1} \sum_{\substack{y_i=1 \\ p^2|Q^*(\mathbf{y})}}^{p^2} a(p\mathbf{y}) + p^{(5n/2)-2} \sum_{\substack{y_i=1 \\ p|Q^*(\mathbf{y})}}^{p} a(p^2\mathbf{y}) \\ &- p^{(3n/2)-1} \sum_{\substack{y_i=1 \\ p^2|Q^*(\mathbf{y})}}^{p^3} a(\mathbf{y}) - p^{2n-2} \sum_{\substack{y_i=1 \\ p|Q^*(\mathbf{y})}}^{p^2} a(p\mathbf{y}) \\ &- p^{(5n/2)-3} \sum_{y_i=1}^{p} a(p^2\mathbf{y}). \end{aligned} \tag{14}$$

If $\Delta = -1$, then

$$\begin{aligned}\sum_{\mathbf{x}\in V_{p^3}} \alpha(\mathbf{x}) &= p^{-3} \sum_{\mathbf{x}} \alpha(\mathbf{x}) - p^{3n/2} \sum_{\substack{y_i=1 \\ p^3|Q^*(\mathbf{y})}}^{p^3} a(\mathbf{y}) \\ &+ p^{2n-1} \sum_{\substack{y_i=1 \\ p^2|Q^*(\mathbf{y})}}^{p^2} a(p\mathbf{y}) - p^{(5n/2)-2} \sum_{\substack{y_i=1 \\ p|Q^*(\mathbf{y})}}^{p} a(p^2\mathbf{y}) \\ &+ p^{(3n/2)-1} \sum_{\substack{y_i=1 \\ p^2|Q^*(\mathbf{y})}}^{p^3} a(\mathbf{y}) - p^{2n-2} \sum_{\substack{y_i=1 \\ p|Q^*(\mathbf{y})}}^{p^2} a(p\mathbf{y}) \\ &+ p^{(5n/2)-3} \sum_{y_i=1}^{p} a(p^2\mathbf{y}). \end{aligned} \tag{15}$$

Auxiliary lemmas

For later reference, we construct the following two lemmas on estimating the sum $\sum_{y_i}^{p^2} a(p\mathbf{y})$ and $\sum_{y_i}^{p} a(p^2\mathbf{y})$. Let $\mathcal{B}$ be a box of points in $\mathbb{Z}^n$ as in (2) centered about the origin with all $m_i \leqslant p^3$, and view this box as a subset of $\mathbb{Z}^n_{p^3}$. Let $\chi_{\mathcal{B}}$ be its characteristic function with Fourier expansion $\chi_{\mathcal{B}}(\mathbf{x}) = \sum_{\mathbf{y}} a_{\mathcal{B}}(\mathbf{y}) e_{p^3}(\mathbf{x}\cdot\mathbf{y})$. Let $\alpha(\mathbf{x}) = \chi_{\mathcal{B}} * \chi_{\mathcal{B}} = \sum_{\mathbf{y}} a(\mathbf{y}) e_{p^3}(\mathbf{x}\cdot\mathbf{y})$. Then for any $\mathbf{y} \in \mathbb{Z}^n_{p^3}$,

$$a(\mathbf{y}) = p^{-3n} \prod_{i=1}^{n} \left(\frac{\sin^2\left(\pi m_i y_i/p^3\right)}{\sin^2\left(\pi y_i/p^3\right)} \right),$$

where the term in the product is taken to be m_i if $y_i = 0$.

Lemma 3. *Let $\mathcal{B}$ be any box of type (2) viewed as a subset of $\mathbb{Z}^n_{p^3}$ and $\alpha(\mathbf{x}) = \chi_{\mathcal{B}} * \chi_{\mathcal{B}}(\mathbf{x})$. Then we have*

$$\sum_{y_i=1}^{p^2} a(p\mathbf{y}) \leqslant \frac{|\mathcal{B}|}{p^n} \prod_{m_i \geqslant p^2} \frac{2m_i}{p^2}.$$

Proof. First,

$$\begin{aligned}\sum_{y_i=1}^{p^2} a(p\mathbf{y}) &= \sum_{y_i=1}^{p^2} \sum_{x_i=1}^{p^3} \frac{1}{p^{3n}} \alpha(\mathbf{x}) e_{p^3}(-\mathbf{x}\cdot p\mathbf{y}) \\ &= \sum_{x_i=1}^{p^3} \frac{1}{p^{3n}} \alpha(\mathbf{x}) \sum_{y_i=1}^{p^2} e_{p^2}(-\mathbf{x}\cdot\mathbf{y}) \\ &= \frac{1}{p^{3n}} \sum_{\substack{x_i=1 \\ \mathbf{x}\equiv 0 \pmod{p^2}}}^{p^2} \alpha(\mathbf{x}) p^{2n} \\ &= \frac{1}{p^n} \sum_{\mathbf{x}\equiv 0 \pmod{p^2}} \alpha(\mathbf{x}) \\ &= \frac{1}{p^n} \sum_{\substack{\mathbf{u}\in\mathcal{B} \\ \mathbf{u}+\mathbf{v}\equiv 0 \pmod{p^2}}} \sum_{\mathbf{v}\in\mathcal{B}} 1. \end{aligned} \tag{16}$$

Now we need to count the number of solutions of the congruence

$$\mathbf{u} + \mathbf{v} \equiv \mathbf{0} \pmod{p^2},$$

with $\mathbf{u}, \mathbf{v} \in \mathcal{B}$. In fact for each choice of $\mathbf{v}$, there are at most $\prod_{i=1}^n([m_i/p^2]+1)$ choices for $\mathbf{u}$. So the total number of solutions is less than or equal to $\prod_{i=1}^n m_i([m_i/p^2]+1)$. It follows from (16),

$$\sum_{y_i=1}^{p^2} a(p\mathbf{y}) \leqslant \frac{1}{p^n} \prod_{i=1}^{n} m_i \left(\left[\frac{m_i}{p^2} \right] + 1 \right). \tag{17}$$

We split the product in (17) to get

$$\prod_{i=1}^{n} m_i \left(\left[\frac{m_i}{p^2} \right] + 1 \right) \leqslant \prod_{m_i < p^2} m_i \prod_{m_i \geqslant p^2} m_i \left(\frac{m_i}{p^2} + 1 \right).$$

Then by help of this inequality we obtain

$$\sum_{y_i=1}^{p^2} a(p\mathbf{y}) \leqslant \frac{1}{p^n} \prod_{m_i<p^2} m_i \prod_{m_i \geqslant p^2} m_i \left(\frac{m_i}{p^2}+1\right) \leqslant \frac{|\mathcal{B}|}{p^n} \prod_{m_i \geqslant p^2} \frac{2m_i}{p^2},$$

proving the lemma. □

Lemma 4. *Let $\mathcal{B}$ be any box of type (2) and $\alpha(\mathbf{x}) = \chi_{\mathcal{B}} * \chi_{\mathcal{B}}(\mathbf{x})$. Then we have*

$$\sum_{y_i=1}^{p} a(p^2\mathbf{y}) \leqslant \frac{|\mathcal{B}|}{p^{2n}} \prod_{m_i \geqslant p} \frac{2m_i}{p}.$$

Proof. The idea of the proof is exactly similar to the ideas used to prove Lemma 3. □

Proof of Theorem 1

Let $\mathcal{B}$ be the box of points in $\mathbb{Z}^n$ given by (2):

$$\mathcal{B} = \{\mathbf{x} \in \mathbb{Z}^n \mid a_i \leqslant x_i < a_i + m_i,\ 1 \leqslant i \leqslant n\}$$

where $a_i, m_i \in \mathbb{Z}$, $1 \leqslant m_i \leqslant p^3$, $1 \leqslant i \leqslant n$. Then $|\mathcal{B}| = \prod_{i=1}^n m_i$, the cardinality of $\mathcal{B}$. View the box $\mathcal{B}$ as a subset of $\mathbb{Z}^n_{p^3}$ and let $\chi_{\mathcal{B}}$ be it characteristic function with Fourier expansion $\chi_{\mathcal{B}}(\mathbf{x}) = \sum_{\mathbf{y}} a_{\mathcal{B}}(\mathbf{y}) e_{p^3}(\mathbf{x}\cdot\mathbf{y})$.

The case $\Delta_p(Q) = -1$:

Consider the congruence (1) and consider (15), the fundamental identity (mod p^3) when $\Delta = -1$:

$$\begin{aligned}\sum_{\mathbf{x}\in V_{p^3}} \alpha(\mathbf{x}) = p^{-3}\sum_{\mathbf{x}} \alpha(\mathbf{x}) \ - \ p^{3n/2} \sum_{\substack{y_i=1 \\ p^3|Q^*(\mathbf{y})}}^{p^3} a(\mathbf{y}) \\ + \ p^{2n-1} \sum_{\substack{y_i=1 \\ p^2|Q^*(\mathbf{y})}}^{p^2} a(p\mathbf{y}) \ - \ p^{(5n/2)-2} \sum_{\substack{y_i=1 \\ p|Q^*(\mathbf{y})}}^{p} a(p^2\mathbf{y}) \\ + \ p^{(3n/2)-1} \sum_{\substack{y_i=1 \\ p^2|Q^*(\mathbf{y})}}^{p^3} a(\mathbf{y}) \ - \ p^{2n-2} \sum_{\substack{y_i=1 \\ p|Q^*(\mathbf{y})}}^{p^2} a(p\mathbf{y}) \\ + \ p^{(5n/2)-3} \sum_{y_i=1}^{p} a(p^2\mathbf{y}).\end{aligned}$$

Put $\alpha = \chi_{\mathcal{B}} * \chi_{\mathcal{B}} = \sum_{\mathbf{y}} a(\mathbf{y}) e_{p^3}(\mathbf{x}\cdot\mathbf{y})$. Then the Fourier coefficients of $\alpha(\mathbf{x})$ are given by $a(\mathbf{y}) = p^{3n} a^2_{\mathcal{B}}(\mathbf{y})$ and by Parseval's identity satisfy

$$\sum_{\mathbf{y}} |a(\mathbf{y})| = p^{3n} \sum_{\mathbf{y}} |a_{\mathcal{B}}(\mathbf{y})|^2 = \sum_{\mathbf{y}} |\chi_{\mathcal{B}}(\mathbf{y})|^2 = |\mathcal{B}|. \tag{18}$$

Consequently from (18),

$$p^{(3n/2)-1} \sum_{\substack{y_i=1 \\ p^2|Q^*(\mathbf{y})}}^{p^3} a(\mathbf{y}) \leqslant p^{3n/2-1} \sum_{\mathbf{y}} |a(\mathbf{y})| \leqslant p^{3n/2-1} |\mathcal{B}|. \tag{19}$$

Besides this we have that the main term in (15) is

$$p^{-3} \sum_{\mathbf{x}} \alpha(\mathbf{x}) = p^{-2} \sum_{\mathbf{x}} \chi_{\mathcal{B}} * \chi_{\mathcal{B}}(\mathbf{x}) = \frac{|\mathcal{B}|^2}{p^3}. \tag{20}$$

Also we have by Lemma 3,

$$p^{2n-1} \sum_{\substack{y_i=1 \\ p^2|Q^*(\mathbf{y})}}^{p^2} a(p\mathbf{y}) \leqslant p^{2n-1} \frac{|\mathcal{B}|}{p^n} \prod_{m_i \geqslant p^2} \frac{2m_i}{p^2} = p^{n-1} |\mathcal{B}| \prod_{m_i \geqslant p^2} \frac{2m_i}{p^2}, \tag{21}$$

and by Lemma 4,

$$p^{(5n/2)-3} \sum_{y_i=1}^{p} a(p^2\mathbf{y}) \leqslant p^{(5n/2)-3} \frac{|\mathcal{B}|}{p^{2n}} \prod_{m_i \geqslant p} \frac{2m_i}{p} = p^{(n/2)-3} |\mathcal{B}| \prod_{m_i \geqslant p} \frac{2m_i}{p}. \tag{22}$$

Now turn back to (15), we have

$$\sum_{\mathbf{x}\in V_{p^3}} \alpha(\mathbf{x}) \leqslant p^{-3} \sum_{\mathbf{x}} \alpha(\mathbf{x}) + p^{(3n/2)-1} \sum_{\substack{y_i=1 \\ p^2|Q^*(\mathbf{y})}}^{p^3} a(\mathbf{y}) + p^{2n-1} \sum_{\substack{y_i=1 \\ p^2|Q^*(\mathbf{y})}}^{p^2} a(p\mathbf{y}) + p^{5n/2-3} \sum_{y_i=1}^{p} a(p^2\mathbf{y}). \tag{23}$$

Then by inequalities in (20), (19), (21), and (22) we obtain

$$\sum_{\mathbf{x}\in V_{p^3}} \alpha(\mathbf{x}) \leqslant \frac{|\mathcal{B}|^2}{p^3} + p^{3n/2-1} |\mathcal{B}| + p^{n-1} |\mathcal{B}| \prod_{m_i \geqslant p^2} \frac{2m_i}{p^2} + p^{(n/2)-3} |\mathcal{B}| \prod_{m_i \geqslant p} \frac{2m_i}{p}. \tag{24}$$

But, it easily to see that

$$\sum_{\mathbf{x}\in V_{p^3}} \alpha(\mathbf{x}) \geqslant \frac{1}{2^n} |\mathcal{B}| \left|V_{p^3} \cap \mathcal{B}\right|. \tag{25}$$

Thus we have (by (24) and (25))

$$\left|V_{p^3} \cap \mathcal{B}\right| = 2^n \left(\frac{|\mathcal{B}|}{p^3} + p^{(3n/2)-1} + p^{n-1} \prod_{m_i \geqslant p^2} \frac{2m_i}{p^2} + p^{(n/2)-3} \prod_{m_i \geqslant p} \frac{2m_i}{p} \right). \tag{26}$$

The task now is designation which of the terms $\frac{|\mathcal{B}|}{p^3}$, $p^{n-1}\prod_{m_i\geqslant p^2}\frac{2m_i}{p^2}$ and $p^{(n/2)-3}\prod_{m_i\geqslant p}\frac{2m_i}{p}$ in (26) is the dominant term. We consider two cases:

Case (i): We define l by

$$m_1\leqslant m_2\leqslant\cdots\leqslant m_l<p^2\leqslant m_{l+1}\leqslant\cdots\leqslant m_n.$$

Then

I. Assume $l\leqslant\frac{n}{2}-1$. Then compare

$$\begin{aligned}\frac{p^{n-1}\prod_{m_i\geqslant p^2}\frac{2m_i}{p^2}}{\frac{1}{p^3}\prod_{i=1}^n m_i}&=\frac{2^{n-l}p^{n+2}}{p^{2(n-l)}\prod_{m_i<p^2}m_i}\\&=\frac{2^{n-l}}{p^{n-2l-2}\prod_{m_i<p^2}m_i}\\&\leqslant\frac{2^{n-l}}{1\cdot 1}\leqslant 2^n,\end{aligned}$$

which leads to

$$p^{n-1}\prod_{m_i\geqslant p^2}^{n}\frac{2m_i}{p^2}\leqslant 2^n\frac{|\mathcal{B}|}{p^3}.$$

II. Assume $l\geqslant\frac{n}{2}$. Then compare

$$\begin{aligned}\frac{p^{n-1}\prod_{m_i\geqslant p^2}\frac{2m_i}{p^2}}{p^{(3n/2)-1}}&=\frac{1}{p^{n/2}}\prod_{m_i\geqslant p^2}\frac{2m_i}{p^2}\\&\leqslant\frac{1}{p^{n/2}}\prod_{m_i\geqslant p^2}2p\\&\leqslant\frac{1}{p^{n/2}}(2p)^{n/2}=2^{n/2},\end{aligned}$$

which implies that

$$p^{n-1}\prod_{m_i\geqslant p^2}^{n}\frac{2m_i}{p^2}\leqslant 2^{n/2}p^{(3n/2)-1}.$$

We get by (I) and (II) that

$$\begin{aligned}p^{n-1}\prod_{m_i\geqslant p^2}\frac{2m_i}{p^2}&\leqslant\max\left(2^n\frac{|\mathcal{B}|}{p^3}\,,\,2^{n/2}p^{(3n/2)-1}\right)\\&\leqslant 2^n\frac{|\mathcal{B}|}{p^3}+2^{n/2}p^{(3n/2)-1}.\end{aligned}$$

Case (ii): We define l' by

$$m_1\leqslant m_2\leqslant\cdots\leqslant m_{l'}<p\leqslant m_{l'+1}\leqslant\cdots\leqslant m_n.$$

Then

III. Assume $l'\leqslant\frac{n}{2}-1$.Then compare

$$\begin{aligned}\frac{p^{(n/2)-3}\prod_{m_i\geqslant p}\frac{2m_i}{p}}{\frac{1}{p^3}\prod_{i=1}^n m_i}&=\frac{2^{n-l'}p^{n/2}}{p^{n-l'}\prod_{m_i<p}m_i}\\&=\frac{2^{n-l'}}{p^{(n/2)-l'}\prod_{m_i<p}m_i}\\&\leqslant\frac{2^n}{p^{n/2}}\left(\frac{p}{2}\right)^{l'}\\&\leqslant\frac{2^n}{p^{n/2}}\left(\frac{p}{2}\right)^{(n/2)-1}\\&\leqslant\frac{2^{(n/2)+1}}{p},\end{aligned}$$

leads to

$$p^{(n/2)-3}\prod_{m_i\geqslant p}^{n}\frac{2m_i}{p}\leqslant\frac{2^{(n/2)+1}}{p}\frac{|\mathcal{B}|}{p^3}.$$

IV. Assume $l'\geqslant\frac{n}{2}$. Then compare

$$\begin{aligned}\frac{p^{(n/2)-3}\prod_{m_i\geqslant p}\frac{2m_i}{p}}{p^{(3n/2)-1}}&=\frac{1}{p^{n+2}}\prod_{m_i\geqslant p}\frac{2m_i}{p}\\&\leqslant\frac{1}{p^{n+2}}\prod_{m_i\geqslant p}2p^2\\&\leqslant\frac{1}{p^{n+2}}(2p^2)^{n-l'}\\&\leqslant\frac{1}{p^{n+2}}(2p^2)^{n/2}=\frac{2^{n/2}}{p^2},\end{aligned}$$

implies that

$$p^{(n/2)-3}\prod_{m_i\geqslant p}^{n}\frac{2m_i}{p}\leqslant\frac{2^{n/2}}{p^2}p^{(3n/2)-1}.$$

Thus by (III) and (IV),

$$p^{(n/2)-3}\prod_{m_i\geqslant p}m_i\leqslant\frac{2^{(n/2)+1}}{p}\frac{|\mathcal{B}|}{p^3}+\frac{2^{n/2}}{p^2}p^{(3n/2)-1}.$$

Together, case (i) and case (ii) gives us

$$\begin{aligned}&p^{n-1}\prod_{m_i\geqslant p^2}\frac{2m_i}{p^2}+p^{(n/2)-3}\prod_{m_i\geqslant p}\frac{2m_i}{p}\\&\leqslant\left(2^n+\frac{2^{(n/2)+1}}{p}\right)\frac{|\mathcal{B}|}{p^3}+\left(2^{n/2}+\frac{2^{n/2}}{p^2}\right)p^{(3n/2)-1}.\end{aligned}$$

We conclude by making use of (26) to get

$$\begin{aligned}\left|V_{p^3}\cap\mathcal{B}\right| &\leqslant 2^n\Bigg(\tfrac{|\mathcal{B}|}{p^3}+p^{(3n/2)-1}+p^{n-1}\prod_{m_i\geqslant p^2}\tfrac{2m_i}{p^2}\\ &\qquad+p^{(n/2)-3}\prod_{m_i\geqslant p}\tfrac{2m_i}{p}\Bigg)\\ &\leqslant 2^n\Big\{\tfrac{|\mathcal{B}|}{p^3}+p^{(3n/2)-1}+\Big(2^n+\tfrac{2^{(n/2)+1}}{p}\Big)\tfrac{|\mathcal{B}|}{p^3}\\ &\qquad+\Big(2^{n/2}+\tfrac{2^{(n/2)}}{p^2}\Big)p^{(3n/2)-1}\Big\}\\ &= 2^n\Big\{\Big[\tfrac{|\mathcal{B}|}{p^3}+\Big(2^n+\tfrac{2^{(n/2)+1}}{p}\Big)\tfrac{|\mathcal{B}|}{p^3}\Big]\\ &\qquad+\Big[p^{(3n/2)-1}+\Big(2^{n/2}+\tfrac{2^{(n/2)}}{p^2}\Big)p^{(3n/2)-1}\Big]\Big\}\\ &= 2^n\Big(1+2^n+\tfrac{2^{(n/2)+1}}{p}\Big)\tfrac{|\mathcal{B}|}{p^3}\\ &\qquad+2^n\Big(1+2^{n/2}+\tfrac{2^{(n/2)}}{p^2}\Big)p^{(3n/2)-1}\\ &\leqslant \upsilon_n'\Big(\tfrac{|\mathcal{B}|}{p^3}+p^{(3n/2)-1}\Big),\end{aligned}$$

where $\upsilon_n' = 2^n\left(1 + 2^n + \frac{2^{(n/2)+1}}{p}\right)$.

The case $\Delta_p(Q) = +1$:

We now examine the case $\Delta = +1$. Appealing to (14), we obtain

$$\begin{aligned}\sum_{\mathbf{x}\in V_{p^3}}\alpha(\mathbf{x}) &\leqslant p^{-3}\sum_{\mathbf{x}}\alpha(\mathbf{x}) + p^{3n/2}\sum_{\substack{y'=1\\ p^3|Q^*(\mathbf{y}')}}^{p^3} a(\mathbf{y}')\\ &\quad+p^{2n-1}\sum_{\substack{y'=1\\ p^2|Q^*(\mathbf{y}')}}^{p^2} a(p\mathbf{y}') + p^{(5n/2)-2}\sum_{\substack{y'=1\\ p|Q^*(\mathbf{y}')}}^{p} a(p^2\mathbf{y}')\\ &\leqslant \frac{|\mathcal{B}|^2}{p^3}+p^{3n/2}|\mathcal{B}|+p^{2n-1}\frac{|\mathcal{B}|}{p^n}\prod_{m_i\geqslant p^2}\frac{2m_i}{p^2}\\ &\quad+p^{(5n/2)-2}\frac{|\mathcal{B}|}{p^{2n}}\prod_{m_i\geqslant p}\frac{2m_i}{p}.\end{aligned}$$

But, once again by (26), we obtain

$$\begin{aligned}\left|V_{p^3}\cap\mathcal{B}\right| = 2^n\Bigg(&\tfrac{|\mathcal{B}|}{p^3}+p^{(3n/2)}+p^{n-1}\prod_{m_i\geqslant p^2}\tfrac{2m_i}{p^2}\\ &+p^{(n/2)-2}\prod_{m_i\geqslant p}\tfrac{2m_i}{p}\Bigg).\end{aligned}\tag{27}$$

We do a similar investigation (as before) to determine which of the quantities $\frac{|\mathcal{B}|}{p^3}$, $p^{3n/2}$, $p^{n-1}\prod_{m_i}\frac{2m_i}{p^2}$ and $p^{(n/2)-2}\prod_{m_i\geqslant p}\frac{2m_i}{p^2}$ of (27) is the dominant term. Indeed in case (i) $l\leqslant \frac{n}{2}-1$, we have (as we saw earlier) $p^{n-1}\prod_{m_i}\frac{2m_i}{p^2}\leqslant 2^n\frac{|\mathcal{B}|}{p^3}$, and when $l\leqslant\frac{n}{2}$,

$$\begin{aligned}\frac{p^{n-1}\prod_{m_i\geqslant p^2}\frac{2m_i}{p^2}}{p^{3n/2}} &= \frac{1}{p^{(n/2)+1}}\prod_{m_i\geqslant p^2}\frac{2m_i}{p^2}\\ &\leqslant \frac{1}{p^{(n/2)+1}}\prod_{m_i\geqslant p^2}2p\\ &\leqslant \frac{1}{p^{(n/2)+1}}(2p)^{n/2} = \frac{2^{n/2}}{p},\end{aligned}$$

which means $p^{n-1}\prod_{m_i}\frac{2m_i}{p^2}\leqslant\frac{2^{n/2}}{p}p^{3n/2}$. We therefore obtain

$$\begin{aligned}p^{n-1}\prod_{m_i\geqslant p^2}\frac{2m_i}{p^2} &\leqslant \max\left(2^n\frac{|\mathcal{B}|}{p^3},\ \frac{2^{n/2}}{p}p^{3n/2}\right)\\ &\leqslant 2^n\frac{|\mathcal{B}|}{p^3}+\frac{2^{n/2}}{p}p^{3n/2}.\end{aligned}$$

In case (ii) when $l'\leqslant\frac{n}{2}-1$, we have

$$\begin{aligned}\frac{p^{(n/2)-2}\prod_{m_i\geqslant p}\frac{2m_i}{p}}{\frac{1}{p^3}\prod_{i=1}^n m_i} &= \frac{2^{n-l'}p^{(n/2)+1}}{p^{n-l'}\prod_{m_i<p}m_i}\\ &= \frac{2^{n-l'}}{p^{(n/2)-l'-1}\prod_{m_i<p}m_i}\\ &\leqslant \frac{2^n}{p^{(n/2)-1}}\left(\frac{p}{2}\right)^{l'}\\ &\leqslant \frac{2^n}{p^{(n/2)-1}}\left(\frac{p}{2}\right)^{(n/2)-1}\\ &\leqslant 2^{(n/2)+1},\end{aligned}$$

which means $p^{(n/2)-2}\prod_{m_i\geqslant p}\frac{2m_i}{p^2}\leqslant\frac{2^{n/2}}{p^2}p^{3n/2}$. When $l'\leqslant\frac{n}{2}$,

$$\begin{aligned}\frac{p^{(n/2)-2}\prod_{m_i\geqslant p}\frac{2m_i}{p}}{p^{3n/2}} &= \frac{1}{p^{n+2}}\prod_{m_i\geqslant p}\frac{2m_i}{p}\\ &\leqslant \frac{1}{p^{n+2}}\prod_{m_i\geqslant p}2p^2\\ &\leqslant \frac{1}{p^{n+2}}(2p^2)^{n-l'}\\ &\leqslant \frac{1}{p^{n+2}}(2p^2)^{n/2} = \frac{2^{n/2}}{p^2},\end{aligned}$$

which means $p^{(n/2)-2}\prod_{m_i\geqslant p}\frac{2m_i}{p}\leqslant\frac{2^{n/2}}{p^2}p^{3n/2}$. Thus we get

$$p^{(n/2)-2}\prod_{m_i\geqslant p}\frac{2m_i}{p}\leqslant 2^{(n/2)+1}\frac{|\mathcal{B}|}{p^3}+\frac{2^{n/2}}{p^2}p^{3n/2}.$$

Putting case (i) and case (ii) together, we obtain

$$\begin{aligned}\left|V_{p^3} \cap \mathcal{B}\right| &\leqslant 2^n \Bigg(\frac{|\mathcal{B}|}{p^3} + p^{(3n/2)} + p^{n-1} \prod_{m_i \geqslant p^2} \frac{2m_i}{p^2} \\ &\qquad + p^{(n/2)-2} \prod_{m_i \geqslant p} \frac{2m_i}{p} \Bigg) \\ &\leqslant 2^n \left\{ \frac{|\mathcal{B}|}{p^3} + p^{(3n/2)} + \left(2^n + 2^{(n/2)+1}\right) \frac{|\mathcal{B}|}{p^3} \right. \\ &\qquad \left. + \left(\frac{2^{n/2}}{p} + \frac{2^{(n/2)}}{p^2} \right) p^{(3n/2)} \right\} \\ &= 2^n \left(1 + 2^n + 2^{(n/2)+1}\right) \frac{|\mathcal{B}|}{p^3} \\ &\qquad + 2^n \left(1 + \frac{2^{n/2}}{p} + \frac{2^{(n/2)}}{p^2}\right) p^{3n/2} \\ &= \upsilon_n'' \left(\frac{|\mathcal{B}|}{p^2} + p^{3n/2} \right),\end{aligned}$$

where $\upsilon_n'' = 2^n (1 + 2^n + 2^{(n/2)+1})$.

Lastly let $\upsilon_n = \upsilon'$ if $\Delta = -1$ and $\upsilon_n = \upsilon''$ if $\Delta = +1$ to conclude the proof of Theorem 1.

Acknowledgements

The author is most grateful to the referee and the editors especially Professor Tin-Yan Tam who handle this paper. He would also like to thank his colleague Professor Idir MECHAI for his assistance in formatting and typesetting this paper.

References

Chalk, J. H. H. (1963). The number of solutions of congruences in incomplete residue systems. *Canad. J. Math*, *15*, 191-296.

Cochrane, T. (1984). Small solutions of congruences. *PhD thesis, Universityof Michigan*.

Cochrane, T. (1989). Small zeros of quadratic congruences (mod p). *J. Number Theory*, *33*(3), 286-292.

Cochrane, T. (1990). Small zeros of quadratic congruences (mod p), II. *Proceedings of the Illinois Number Theory Conference (1989)*, *33*(3), 91-94. (Birkhäuser, Boston)

Cochrane, T. (1991). Small zeros of quadratic congruences (mod p), III. *J. Number Theory*, *33*(1), 92-99.

Cochrane, T., & Hakami, A. (2012). Small zeros of quadratic congruences (mod p^2). *Proceedings of the American Mathematical Society*, *140*(12), 4041-4052.

Hakami, A. (2009). Small zeros of quadratic congruences to a prime power modulus. *PhD thesis, Kansas State University*.

Hakami, A. (2011a). On Cochrane's estimate for small zeros of quadratic forms (mod p). *Far East J. Math. Sci.*, *50*(2), 151-157.

Hakami, A. (2011b). Small zeros of quadratic forms (mod p^2). *JP J. Algebra Number Theory Appl.*, *17*(2), 141-162.

Hakami, A. (2011c). Small zeros of quadratic forms (mod p^3). *Adv. Appl. Math. Sci.*, *9*(1), 47-69.

Hakami, A. (2012). Weighted quadratic partitions (*mod* p^m) , a new formula and new demonstration. *Tamaking J. Math.*, *43*(1), 11-19.

Hakami, A. (2014a). Estimates for lattice points of quadratic forms with integral coefficients modulo a prime number square. *Journal of Inequalities and Applications*. doi: 10.1186/1029-242X-2014-290

Hakami, A. (2014b). Small zeros of quadratic forms (mod p^m). *Ramanujan J*. doi: 10.1007/s11139-014-9614-3

Hakami, A. (2015). Estimates for lattice points of quadratic forms with integral coefficients modulo a prime number square II. *Journal of Inequalities and Applications*. doi: 10.1186/s13660-015-0637-0

Heath-Brown, D. R. (1985). Small solutions of quadratic congruences. *Glasgow Math. J*, *27*.

Heath-Brown, D. R. (1991). Small solutions of quadratic congruences, II. *Mathematika*, *38*(2).

Myerson, G. (1991). The distribution of rational points on varieties defined over a finite field. *Mathematika*, *28*, 153-159.

Schinzel, A., Schlickewei, H. P., & Schmidt, W. M. (1980). Small solutions of quadratic congruences and small fractional parts of quadratic forms. *Acta Arith*, *37*, 241-248.

Tietäväinen, A. (1967). On the solvability of equations in incomplete finite fields. *Ann. Unviv. Turku. Ser. AI*, *102*, 1-13.

Wang, Y. (1989). On small zeros of quadratic forms over finite fields. *J. Number Theory*, *31*, 272-284. (World Sci. Publ., Teaneck, NJ)

Wang, Y. (1990). On small zeros of quadratic forms over finite fields. *Algebraic structures and number theory, (Hong Kong, 1988)*, 269-274. (World Sci. Publ., Teaneck, NJ)

Wang, Y. (1993). On small zeros of quadratic forms over finite fields II. *Acta Math. Sinica (N.S.)*, *9*(4), 382-389. (A Chinese summary appears in Acta Math. Sinica, (37) (5) (1994), 719-720)