JP Journal of Algebra, Number Theory and Applications
Volume 21, Number 2, 2011, Pages 133-155
Published Online: May 26, 2011
This paper is available online at http://pphmj.com/journals/jpanta.htm

THE NUMBER OF INTEGRAL POINTS OF QUADRATIC FORMS MODULO p^2

ALI H. HAKAMI

Department of Mathematics
King Khalid University
P. O. Box 9004, Abha
Postal Code: 61431, Saudi Arabia
e-mail: aalhakami@kku.edu.sa

Abstract

Let $Q(\mathbf{x}) = Q(x_1, x_2, ..., x_n)$ be a quadratic form over $\mathbb{Z}$ and p be an odd prime. Let $V = V_Q = V_{p^2}$ denote the set of zeros of $Q(\mathbf{x})$ in $\mathbb{Z}_{p^2}$ and $|V|$ denote the cardinality of V. Set $\phi(V_{p^2}, \mathbf{y}) = \sum_{\mathbf{x}\in V} e_{p^2}(\mathbf{x}\cdot\mathbf{y})$ for $\mathbf{y} \neq \mathbf{0}$ and $\phi(V_{p^2}, \mathbf{y}) = |V_p| - p^{2(n-1)}$ for $\mathbf{y} = \mathbf{0}$. In this paper, we are interested to determine the number of integer solutions of the congruence $Q(\mathbf{x}) \equiv 0 \pmod{p^2}$.

1. Introduction

Let $Q(\mathbf{x}) = Q(x_1, x_2, ..., x_n) = \sum_{1\le i\le j\le n} a_{ij}x_ix_j$ be a quadratic form with integer coefficients in n-variables and $V = V_{p^2}(Q)$ be the algebraic subset of $\mathbb{Z}^n_{p^2}$ defined by the equation $Q(\mathbf{x}) = 0$. When n is even, we let $\Delta_p(Q) = ((-1)^{n/2} \det A_Q / p)$ if $p \nmid \det A_Q$ and $\Delta_p(Q) = 0$ if $p | \det A_Q$, where $(\bullet/p)$

2010 Mathematics Subject Classification: 11D79.

Keywords and phrases: quadratic forms, integer solutions.

Received December 19, 2010

denotes the Legendre-Jacobi symbol and A_Q is the $n \times n$ defining matrix for $Q(\mathbf{x})$. Our interest in this paper is in the problem of finding points in V with the variables restricted to a box of the type

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

where $a_i,\ m_i \in \mathbb{Z},$ and $0 < m_i < p^2$ for $1 \le i \le n.$ Consider the congruence

$$Q(\mathbf{x}) \equiv 0 \pmod{p^2}. \tag{2}$$

The final result of this pepper is stated in the following theorem.

Theorem 1. *Let* $V_{p^2,\mathbb{Z}} = V_{p^2,\mathbb{Z}}(Q)$ *be the set of integer solutions of the congruence* (2). *Then for any box* $\mathscr{B}$ *of type* (1),

$$|\mathscr{B} \cap V_{p^2,\mathbb{Z}}| \le \gamma_n\left(\frac{|\mathscr{B}|}{p^2} + N_{\mathscr{B}} p^n\right), \tag{3}$$

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

$$\gamma_n = 2^n(1 + 6^n), \tag{4}$$

and we define

$$N_{\mathscr{B}} = \prod_{i=1}^{n}\left(\left[\frac{m_i}{p^2}\right] + 1\right). \tag{5}$$

We shall devote the rest of Section 4 to give the proof of Theorem 1. If V is the set of zeros of a "nonsingular" quadratic form $Q(\mathbf{x}),$ then we can show that

$$|V \cap \mathscr{B}| = \frac{|\mathscr{B}|}{p} + O(p^{n/2}(\log p)^{2n}), \tag{6}$$

for any box $\mathscr{B}$ (see [1] and [7]). It is apparent from (6) that $|V \cap \mathscr{B}|$ is nonempty provided

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

For any $\mathbf{x}, \mathbf{y}$ in $\mathbb{Z}^n_{p^2}$, let $\mathbf{x} \cdot \mathbf{y}$ denote the ordinary dot product, $\mathbf{x} \cdot \mathbf{y} =$

$\sum_{i=1}^{n} x_i y_i$. For any $x \in \mathbb{Z}_{p^2}$, let $e_{p^2}(x) = e^{2\pi i x/p^2}$. We use the abbreviation $\sum_{\mathbf{x}} = \sum_{\mathbf{x} \in \mathbb{Z}_{p^2}^n}$ for complete sums. The key ingredient in obtaining the identity in (6) is a uniform upper bound on the function

$$\phi(V, \mathbf{y}) = \begin{cases} \sum_{\mathbf{x} \in V} e_{p^2}(\mathbf{x} \cdot \mathbf{y}) & \text{for } \mathbf{y} \neq \mathbf{0}, \\ |V| - p^{2(n-1)} & \text{for } \mathbf{y} = \mathbf{0}. \end{cases} \tag{7}$$

In order to show that $\mathscr{B} \cap V$ is nonempty we can proceed as follows. Let $\alpha(\mathbf{x})$ be a complex valued function on $\mathbb{Z}_{p^2}^n$ such that $\alpha(\mathbf{x}) \leq 0$ for all $\mathbf{x}$ not in $\mathscr{B}$. If we show that $\sum_{\mathbf{x} \in V} \alpha(\mathbf{x}) > 0$, then it will follow that $\mathscr{B} \cap V$ is nonempty. Now $\alpha(\mathbf{x})$ has a finite Fourier expansion

$$\alpha(\mathbf{x}) = \sum_{\mathbf{y}} a(\mathbf{y}) e_{p^2}(\mathbf{y} \cdot \mathbf{x}),$$

where

$$a(\mathbf{y}) = p^{-n} \sum_{\mathbf{x}} \alpha(\mathbf{x}) e_{p^2}(-\mathbf{y} \cdot \mathbf{x}),$$

for all $\mathbf{y} \in \mathbb{Z}_{p^2}^n$. Thus

$$\begin{aligned} \sum_{\mathbf{x} \in V} \alpha(\mathbf{x}) &= \sum_{\mathbf{x} \in V} \sum_{\mathbf{y}} a(\mathbf{y}) e_{p^2}(\mathbf{y} \cdot \mathbf{x}) \\ &= \sum_{\mathbf{y}} a(\mathbf{y}) \sum_{\mathbf{x} \in V} e_{p^2}(\mathbf{y} \cdot \mathbf{x}) \\ &= a(\mathbf{0}) |V| + \sum_{\mathbf{y} \neq 0} a(\mathbf{y}) \sum_{\mathbf{x} \in V} e_{p^2}(\mathbf{y} \cdot \mathbf{x}). \end{aligned}$$

Since $a(\mathbf{0}) = p^{-2n} \sum_{\mathbf{x}} \alpha(\mathbf{x})$, we obtain

$$\sum_{\mathbf{x} \in V} \alpha(\mathbf{x}) = p^{-2n} |V| \sum_{\mathbf{x}} \alpha(\mathbf{x}) + \sum_{\mathbf{y} \neq 0} a(\mathbf{y}) \phi(V, \mathbf{y}), \tag{8}$$

where $\phi(V, \mathbf{y})$ is defined by (7). A variation of (8) that is sometimes more useful is

$$\sum_{\mathbf{x}\in V} \alpha(\mathbf{x}) = p^{-2} \sum_{\mathbf{x}} \alpha(\mathbf{x}) + \sum_{\mathbf{y}} a(\mathbf{y}) \phi(V, \mathbf{y}), \tag{9}$$

which is obtained from (8) by noticing that $|V| = \phi(V, \mathbf{0}) + p^{2(n-1)}$, whence

$$\sum_{\mathbf{x}\in V} \alpha(\mathbf{x}) = a(\mathbf{0})[\phi(V, \mathbf{0}) + p^{2(n-1)}] + \sum_{\mathbf{y}\neq 0} a(\mathbf{y}) \phi(V, \mathbf{y}),$$

$$= p^{2n-2} a(\mathbf{0}) + \sum_{\mathbf{y}} a(\mathbf{y}) \phi(V, \mathbf{y}).$$

Equations (8) and (9) 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, $|V| \approx p^{2(n-1)}$ 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 $|V| = p^{2(n-1)} + O(p^n)$ (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 (8) or (9). We try to make an optimal choice of $\alpha(\mathbf{x})$ in order to minimize the error term. Special cases of (8) and (9) have appeared a number of times in the literature for different types of algebraic sets V; Chalk [4], Tietäväinen [6] and Myerson [5]. The first case treated was to let $\alpha(\mathbf{x})$ be the characteristic function $\chi_S(\mathbf{x})$ of a subset S of $\mathbb{Z}^n_{p^2}$, whence (9) gives rise to formulas of the type

$$|V \cap S| = p^{-2}|S| + \textit{Error}.$$

Equation (2) is obtained in this manner. Particular attention has been given to the case where $S = \mathcal{B}$, a box of points in $\mathbb{Z}^n_{p^2}$. Another popular choice for α is let it be a convolution of two characteristic functions, $\alpha = \chi_S * \chi_T$ for $S, T \subseteq \mathbb{Z}^n_{p^2}$. We recall that if $\alpha(\mathbf{x}), \beta(\mathbf{x})$ are complex valued functions defined on $\mathbb{Z}^n_{p^2}$, 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 $\mathbf{x} \in \mathbb{Z}^n_{p^2}$. 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, $(S + T) \bigcap V$ 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,

$$\sum_{\mathbf{x}\in\mathbb{Z}^n_{p^2}} e_{p^2}(\mathbf{x} \cdot \mathbf{y}) = \begin{cases} p^{2n} & \text{if } \mathbf{y} = \mathbf{0}, \\ 0 & \text{if } \mathbf{y} \neq \mathbf{0}, \end{cases}$$

and can be routinely checked. By viewing $\mathbb{Z}^n_{p^2}$ as a $\mathbb{Z}$ -module, the Gauss sum

$$S_p(Q, \mathbf{y}) = \sum_{\mathbf{x}\in\mathbb{Z}^n_{p^2}} e_{p^2}(Q(\mathbf{x}) + \mathbf{y} \cdot \mathbf{x}),$$

is well defined whether we take $\mathbf{y} \in \mathbb{Z}^n$ or $\mathbf{y} \in \mathbb{Z}^n_{p^2}$. Let $\alpha(\mathbf{x})$, $\beta(\mathbf{x})$ be complex valued functions on $\mathbb{Z}^n_{p^2}$ with the Fourier expansions

$$\alpha(\mathbf{x}) = \sum_{\mathbf{y}} a(\mathbf{y}) e_{p^2}(\mathbf{x} \cdot \mathbf{y}), \qquad \beta(\mathbf{x}) = \sum_{\mathbf{y}} b(\mathbf{y}) e_{p^2}(\mathbf{x} \cdot \mathbf{y}).$$

Then

$$\alpha * \beta(\mathbf{x}) = \sum_{\mathbf{y}} p^{2n} a(\mathbf{y}) b(\mathbf{y}) e_{p^2}(\mathbf{x} \cdot \mathbf{y}), \tag{10}$$

$$\alpha\beta(\mathbf{x}) = \alpha(\mathbf{x})\beta(\mathbf{x}) = \sum_{\mathbf{y}} (a * b)(\mathbf{y}) e_{p^2}(\mathbf{x} \cdot \mathbf{y}), \tag{11}$$

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

$$\sum_{\mathbf{x}} |(\alpha * \beta)(\mathbf{x})| \le \left(\sum_{\mathbf{x}} |\alpha(\mathbf{x})|\right)\left(\sum_{\mathbf{x}} |\beta(\mathbf{x})|\right), \tag{13}$$

$$\sum_{\mathbf{y}} |a(\mathbf{y})|^2 = p^{-2n} \sum_{\mathbf{x}} |\alpha(\mathbf{x})|^2. \tag{14}$$

The last identity is Parseval's equality.

2. 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 (2):

$$Q(\mathbf{x}) \equiv 0 \pmod{p^2}.$$

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

Lemma 1 [2, Lemma 2.3]**.** *Suppose n is even, Q is nonsingular modulo p and $\Delta = \Delta_p(Q)$. For $\mathbf{y} \in \mathbb{Z}^n$, put $\mathbf{y}' = \frac{1}{p}\mathbf{y}$ in case $p \mid \mathbf{y}$. Then for any $\mathbf{y}$,*

$$\phi(V, \mathbf{y}) = \begin{cases} p^n - p^{n-1} & \text{if } p \nmid y_i \text{ for some } i \text{ and } p^2 \mid Q^*(\mathbf{y}), \\ -p^{n-1} & \text{if } p \nmid y_i \text{ for some } i \text{ and } p \| Q^*(\mathbf{y}), \\ 0 & \text{if } p \nmid y_i \text{ for some } i \text{ and } p \nmid Q^*(\mathbf{y}), \\ -\Delta p^{(3n/2)-2} + p^{n-1}(p-1) & \text{if } p \mid y_i \text{ for all } i \text{ and } p \nmid Q^*(\mathbf{y}'), \\ \Delta(p-1)p^{(3n/2)-2} + p^{n-1}(p-1) & \text{if } p \mid y_i \text{ for all } i \text{ and } p \mid Q^*(\mathbf{y}'), \end{cases}$$

where Q^* is the quadratic form associated with the inverse of the matrix for $Q \bmod p$.

Back to (14) we saw the identity

$$\sum_{\mathbf{x} \in V} \alpha(\mathbf{x}) = p^{-2} \sum_{\mathbf{x}} \alpha(\mathbf{x}) + \sum_{\mathbf{y} \neq 0} a(\mathbf{y}) \phi(V, \mathbf{y}).$$

Inserting the value $\phi(V, \mathbf{y})$ in Lemma 1 yields (see [3]),

Lemma 2 [The fundamental identity]**.** *For any complex valued* $\alpha(\mathbf{x})$ *on* $\mathbb{Z}^n_{p^2}$,

$$\sum_{\mathbf{x}\in V}\alpha(\mathbf{x}) = p^{-2}\sum_{\mathbf{x}}\alpha(\mathbf{x}) + p^n \sum_{p^2 \mid Q^*(\mathbf{y})} a(\mathbf{y}) - p^{n-1} \sum_{p \mid Q^*(\mathbf{y})} a(\mathbf{y})$$

$$- \Delta p^{(3n/2)-2} \sum_{\mathbf{y}'(\mathrm{mod}\ p)}^{p} a(p\mathbf{y}') + \Delta p^{(3n/2)-1} \sum_{\substack{p \mid Q^*(\mathbf{y}') \\ \mathbf{y}'(\mathrm{mod}\ p)}} a(p\mathbf{y}'). \qquad (15)$$

3. Auxiliary Lemma on Estimating the Sum $\sum_{y_i=1}^{p} a(py)$

For later reference, we construct the following lemma on estimating the sum $\sum_{y_i=1}^{p} a(p\mathbf{y})$. Let $\mathscr{B}$ be a box of points in $\mathbb{Z}^n$ as in (1) centered about the origin with all $m_i \le p^2$, and view this box as a subset of $\mathbb{Z}^n_{p^2}$. Let $\chi_{\mathscr{B}}$ be its characteristic function with the Fourier expansion $\chi_{\mathscr{B}}(\mathbf{x}) = \sum_{\mathbf{y}} a_{\mathscr{B}}(\mathbf{y}) e_{p^2}(\mathbf{x}\cdot\mathbf{y})$. Let $\alpha(\mathbf{x}) = \chi_{\mathscr{B}} * \chi_{\mathscr{B}} = \sum_{\mathbf{y}} a(\mathbf{y}) e_{p^2}(\mathbf{x}\cdot\mathbf{y})$. Then for any $\mathbf{y} \in \mathbb{Z}^n_{p^2}$,

$$a(\mathbf{y}) = p^{-2n} \prod_{i=1}^{n} \frac{\sin^2 \pi m_i y_i / p^2}{\sin^2 \pi y_i / p^2}, \qquad (16)$$

where the term in the product is taken to be m_i if $y_i = 0$. In particular, if we take $|y_i| \le p^2/2$ for all *i*, then

$$a(\mathbf{y}) \le p^{-2n} \prod_{i=1}^{n} \min\left\{ m_i^2, \left(\frac{p^2}{2y_i}\right)^2 \right\}.$$

Lemma 3. *Let* $\mathscr{B}$ *be any box of type* (1) *and* $\alpha(\mathbf{x}) = \chi_{\mathscr{B}} * \chi_{\mathscr{B}}(\mathbf{x})$. *Suppose*

$$m_1 \le m_2 \le \cdots \le m_l < p \le m_{l+1} \le \cdots \le m_n. \qquad (17)$$

Then

$$\sum_{\mathbf{y}\in\mathbb{Z}_p^n} a(p\mathbf{y}) \le 2^{n-l} p^{l-2n} |\mathscr{B}| \prod_{i=l+1}^{n} m_i.$$

Proof. We first observe that

$$\sum_{y=1}^{p} a(p\mathbf{y}) = \sum_{y_i=1}^{p}\sum_{x_i=1}^{p^2} \frac{1}{p^{2n}}\alpha(\mathbf{x})e_{p^2}(-\mathbf{x}\cdot p\mathbf{y})$$

$$= \sum_{x_i=1}^{p^2} \frac{1}{p^{2n}}\alpha(\mathbf{x})\sum_{y_i=1}^{p} e_p(-\mathbf{x}\cdot\mathbf{y})$$

$$= \sum_{\substack{x_i=1 \\ x\equiv 0 \pmod p}}^{p^2} \frac{p^n}{p^{2n}}\alpha(\mathbf{x})$$

$$= \frac{1}{p^n}\sum_{x\equiv 0 \pmod p}\alpha(\mathbf{x})$$

$$= \frac{1}{p^n}\sum_{\substack{\mathbf{u}\in\mathscr{B} \\ \mathbf{u}+\mathbf{v}\equiv 0 \pmod p}}\ \sum_{\mathbf{v}\in\mathscr{B}} 1$$

$$\le \frac{1}{p^n}\prod_{i=1}^{n} m_i\left(\left[\frac{m_i}{p}\right]+1\right). \tag{18}$$

To obtain the last inequality in (18) we must count the number of solutions of the congruence

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

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

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

Using the hypothesis (17) then continuing from (18), we have

$$\sum_{y_i=1}^{p} a(p\mathbf{y}) \le \frac{1}{p^n}\prod_{i=1}^{l} m_i \prod_{i=l+1}^{n} m_i\left(\frac{m_i}{p}+1\right)$$

$$\le \frac{|\mathscr{B}|}{p^n}\prod_{i=l+1}^{n}\left(\frac{2m_i}{p}\right) \le \frac{2^{n-l}|\mathscr{B}|}{p^{2n-l}}\prod_{i=l+1}^{n} m_i.$$

The lemma is established. □

Another way to derive a good estimate for the sum $\sum_{y_i}^{p} a(p\mathbf{y})$ is as the following: Let $\mathbf{y}'$ run through the set $\{y' \in \mathbb{Z}_p : Q^*(\mathbf{y}') \equiv 0 \pmod p\}$. Rewrite (16) to be for any $\mathbf{y} \in \mathbb{Z}_{p^2}^n$, with $|y_i| < p/2$,

$$a(\mathbf{y}) = \prod_{i=1}^{n} a_i(y_i),$$

where

$$a_i(y_i) = \frac{1}{p^2} \frac{\sin^2 \pi m_i y_i / p^2}{\sin^2 \pi y_i / p^2},$$

and the term in the product is taken to be m_i if $y_i = 0$ (as before). Then plainly

$$|a_i(y_i)| \le \frac{1}{p^2} \min\left\{m_i^2, \frac{p^4}{4y_i^2}\right\} = \min\left\{\left(\frac{m_i}{p}\right)^2, \frac{p^2}{4y_i^2}\right\}. \tag{19}$$

Replace each $\mathbf{y}$ by $p\mathbf{y}'$. Then, with $|y_i'| < p/2$, we have

$$|a(py_i')| \le \min\left\{\left(\frac{m_i}{p}\right)^2, \frac{1}{4y_i'^2}\right\}.$$

Thus

$$\sum_{y_i}^{p} |a(p\mathbf{y})| \le \sum_{\substack{\mathbf{y} \\ 1 \le y_i \le p}} \prod_{i=1}^{n} |a_i(py_i)| = \prod_{i=1}^{n} \sum_{|y_i| < p/2} |a_i(py_i)|$$

$$\le \prod_{i=1}^{n} \sum_{|y_i| < p/2} \min\left\{\frac{m_i^2}{p^2}, \frac{1}{4y_i^2}\right\}$$

$$\le \prod_{i=1}^{n} \left[\sum_{|y_i| \le p/2m_i} \frac{m_i^2}{p^2} + \sum_{|y_i| > p/2m_i} \frac{1}{4y_i^2}\right]$$

(using the fact: $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$ and continuing),

$$\le \prod_{i=1}^{n} \left[\left(\frac{p}{m_i} + 1\right)\frac{m_i^2}{p^2} + \frac{1}{4} 2 \frac{\pi^2}{6}\right] = \prod_{i=1}^{n} \left(\frac{m_i}{p} + \frac{m_i^2}{p^2} + 1\right).$$

Assuming (17), we have

$$\sum_{\mathbf{y}} |\, a(p\mathbf{y})\,| \le \prod_{i=1}^{l} 3 \prod_{i=l+1}^{n} 3\left(\frac{m_i^2}{p^2}\right) = 3^n \prod_{i=l+1}^{n}\left(\frac{m_i^2}{p^2}\right).$$

Comparing the above two estimates for $\sum_{y_i}^{p} a(p\mathbf{y}),$ we conclude that the estimate the first one is still better.

4. Lattice Points in the Box $\mathscr{B}$

As we mentioned before our interest in this paper is in determining the number of solutions of the congruence (2):

$$Q(\mathbf{x}) \equiv 0 \pmod{p^2},$$

with $x \in \mathscr{B},$ the box of points in $\mathbb{Z}^n$ given by (1):

$$\mathscr{B} = \{\mathbf{x} \in \mathbb{Z}^n \,|\, a_i \le x_i < a_i + m_i, 1 \le i \le n\},$$

where $a_i, m_i \in \mathbb{Z}, 1 \le m_i \le p^2, 1 \le i \le n.$ Then $|\mathscr{B}| = \prod_{i=1}^{n} m_i,$ the cardinality of $\mathscr{B}.$ View the box $\mathscr{B}$ as a subset of $\mathbb{Z}^n_{p^2}$ and let $\chi_{\mathscr{B}}$ be its characteristic function with the Fourier expansion

$$\chi_{\mathscr{B}}(\mathbf{x}) = \sum_{\mathbf{y}} a_{\mathscr{B}}(\mathbf{y}) e_{p^2}(\mathbf{x} \cdot \mathbf{y}).$$

Lemma 4. *Let p be an odd prime, $V_{p^2} = V_{p^2}(Q)$ be the set of zeros of* (2) *in* $\mathbb{Z}^n_{p^2}$, *and* $\mathscr{B}$ *be a box as given in* (1) *centered at the origin with all* $m_i \le p^2$. *If* $\Delta_p = \pm 1,$ *then*

$$|\, \mathscr{B} \cap V_{p^2} \,| \le \vartheta_n\left(\frac{|\mathscr{B}|}{p^2} + p^n\right),$$

where

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

Proof. We begin by writing (15), the fundamental identity $(\mathrm{mod}\ p^2)$:

$$\sum_{\mathbf{x}\in V_{p^2}} \alpha(\mathbf{x}) = p^{-2}\sum_{\mathbf{x}} \alpha(\mathbf{x}) + p^n \sum_{\substack{y_i=1 \\ p^2 \mid Q^*(\mathbf{y})}}^{p^2} a(\mathbf{y}) - p^{n-1} \sum_{\substack{y_i=1 \\ p \mid Q^*(\mathbf{y})}}^{p^2} a(\mathbf{y})$$

$$- \Delta p^{(3n/2)-2} \sum_{y_i'=1}^{p} a(p\mathbf{y}') + \Delta p^{(3n/2)-1} \sum_{\substack{y_i'=1 \\ p \mid Q^*(\mathbf{y}')}}^{p} a(p\mathbf{y}').$$

Set $\alpha = \chi_{\mathscr{B}} * \chi_{\mathscr{B}} = \sum_{\mathbf{y}} a(\mathbf{y}) e_{p^2}(\mathbf{x}\cdot\mathbf{y})$. Then the Fourier coefficients of $\alpha(\mathbf{x})$ are given by $a(\mathbf{y}) = p^{2n} a_{\mathscr{B}}^2(\mathbf{y})$ and since $\mathscr{B}$ is centered at the origin, these are positive real numbers. By Parseval's identity, we have

$$\sum_{\mathbf{y}} |\, a(\mathbf{y})\,| = p^{2n} \sum_{\mathbf{y}} |\, a_{\mathscr{B}}(\mathbf{y})\,|^2 = \sum_{\mathbf{y}} |\, \chi_{\mathscr{B}}(\mathbf{y})\,|^2 = |\, \mathscr{B}\,|. \tag{20}$$

Thus, it follows from (20),

$$p^n \sum_{\substack{y_i=1 \\ p^2 \mid Q^*(\mathbf{y})}}^{p^2} a(\mathbf{y}) \le p^n \sum_{\mathbf{y}} |\, a(\mathbf{y})\,| \le p^n |\, \mathscr{B}\,|. \tag{21}$$

Notice that the main term in (15) is

$$p^{-2}\sum_{\mathbf{x}} \alpha(\mathbf{x}) = p^{-2}\sum_{\mathbf{x}} \chi_{\mathscr{B}} * \chi_{\mathscr{B}}(x) = \frac{|\, \mathscr{B}\,|^2}{p^2}. \tag{22}$$

By Lemma 3, we have

$$p^{(3n/2)-2} \sum_{y_i'=1}^{p} a(p\mathbf{y}') \le 2^{n-l}\, p^{l-(n/2)-2} |\, \mathscr{B}\,| \prod_{i=l+1}^{n} m_i, \tag{23}$$

and

$$p^{(3n/2)-1} \sum_{\substack{y_i'=1 \\ p \mid Q^*(\mathbf{y}')}}^{p} a(p\mathbf{y}') \le p^{(3n/2)-1} \sum_{\mathbf{y}'} a(p\mathbf{y}') \le 2^{n-l}\, p^{l-(n/2)-1} |\, \mathscr{B}\,| \prod_{i=l+1}^{n} m_i, \tag{24}$$

where l, as defined before,

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

The case $\Delta_p(Q) = -1$**.**

Now going back to (15), if $\Delta = -1$, then we have

$$\sum_{\mathbf{x}\in V_{p^2}} \alpha(\mathbf{x}) \le p^{-2}\sum_{\mathbf{x}} \alpha(\mathbf{x}) + p^n \sum_{\substack{y_i=1 \\ p^2 \mid Q^*(\mathbf{y})}}^{p^2} a(\mathbf{y}) + p^{(3n/2)-2}\sum_{y_i'=1}^{p} a(p\mathbf{y}'). \qquad (25)$$

Then by the equalities in (21), (22) and (23), we obtain

$$\sum_{\mathbf{x}\in V_{p^2}} \alpha(\mathbf{x}) \le \underbrace{\frac{|\mathscr{B}|^2}{p^2}}_{①} + \underbrace{p^n|\mathscr{B}|}_{②} + \underbrace{2^{n-l}p^{l-(n/2)-2}|\mathscr{B}|\prod_{i=l+1}^{n} m_i}_{③}. \qquad (26)$$

We next determine which of the terms ①, ② and ③ in (26) is the dominant term. We consider two cases:

Case (i). Suppose $l \le \frac{n}{2} - 1$. Then compare

$$\frac{③}{①} = \frac{2^{n-l}p^{l-(n/2)-2}|\mathscr{B}|\prod_{i=l+1}^{n} m_i}{|\mathscr{B}|^2/p^2}$$

$$= \frac{1}{|\mathscr{B}|}p^{l-(n/2)}2^{n-l}\prod_{i=l+1}^{n} m_i = \frac{p^{l-(n/2)}2^{n-l}}{\prod_{i=1}^{l} m_i}$$

$$\le 2^{n-l}p^{l-(n/2)} = 2^n\left(\frac{p}{2}\right)^l p^{-n/2} \le 2^n\left(\frac{p}{2}\right)^{(n/2)-1} p^{-n/2} \le 2^{(n/2)+1}\cdot\frac{1}{p},$$

which implies that

$$③ \le \frac{2^{(n/2)+1}}{p}① \quad \text{or} \quad 2^n p^{l-(n/2)-2}|\mathscr{B}|\prod_{i=l+1}^{n} m_i \le \frac{2^{(n/2)+1}}{p}\frac{|\mathscr{B}|^2}{p^2}.$$

Case (ii). Suppose $l \ge \frac{n}{2}$. Then compare

$$\frac{③}{②} = \frac{2^{n-l}p^{l-(n/2)-2}|\mathscr{B}|\prod_{i=l+1}^{n} m_i}{p^n|\mathscr{B}|} = 2^{n-l}p^{l-(3n/2)-2}\prod_{i=l+1}^{n} m_i$$

$$\le 2^n p^{l-(3n/2)-2}p^{2(n-l)} = 2^{n-l}p^{n/2-2-l} \le \frac{2^{n/2}}{p^2},$$

which leads to

$$③ \le \frac{2^{n/2}}{p^2}② \quad \text{or} \quad 2^n p^{l-(n/2)-2}|\mathscr{B}|\prod_{i=l+1}^{n} m_i \le \frac{2^{n/2}}{p^2} p^n |\mathscr{B}|.$$

So for any l, we have

$$③ \le \left(\frac{2^{(n/2)+1}}{p}① + \frac{2^{n/2}}{p^2}②\right)$$

or

$$2^{n-l} p^{l-(n/2)-2}|\mathscr{B}|\prod_{i=l+1}^{n} m_i \le \left(\frac{2^{(n/2)+1}}{p}\frac{|\mathscr{B}|^2}{p^2} + \frac{2^{n/2}}{p^2} p^n |\mathscr{B}|\right).$$

Returning to (26), we now write

$$\begin{aligned}\sum_{\mathbf{x}\in V_{p^2}} \alpha(\mathbf{x}) &\le ① + ② + ③ \\ &\le ① + ② + \frac{2^{(n/2)+1}}{p}① + \frac{2^{n/2}}{p^2}② \\ &= \left(1 + \frac{2^{(n/2)+1}}{p}\right)① + \left(1 + \frac{2^{n/2}}{p^2}\right)② \\ &\le \vartheta_n'\left(\frac{|\mathscr{B}|^2}{p^2} + p^n|\mathscr{B}|\right), \end{aligned} \tag{27}$$

where $\vartheta_n' = 1 + (2^{(n/2)+1}/p)$. On the other hand,

$$\sum_{\mathbf{x}\in V_{p^2}} \alpha(\mathbf{x}) \ge \frac{1}{2^n}|\mathscr{B}||V_{p^2} \cap \mathscr{B}|. \tag{28}$$

Hence, it follows by combining (27) and (28) that

$$|\mathscr{B} \cap V_{p^2}| \le 2^n \vartheta_n'\left(\frac{|\mathscr{B}|}{p^2} + p^n\right).$$

The case $\Delta_p(Q) = +1$**.**

If $\Delta_p = +1$, again by (15), we have

$$\sum_{\mathbf{x}\in V_{p^2}} \alpha(\mathbf{x}) \le p^{-2}\sum_{\mathbf{x}} \alpha(\mathbf{x}) + p^n \sum_{\mathbf{y}} |\, a(\mathbf{y})\,| + p^{(3n/2)-1} \sum_{\mathbf{y} (\mathrm{mod}\ p)} a(p\mathbf{y})$$

$$\le \underbrace{\frac{|\,\mathscr{B}\,|^2}{p^2}}_{①} + \underbrace{p^n |\,\mathscr{B}\,|}_{②} + \underbrace{2^{n-l}\, p^{l-(n/2)-1} |\,\mathscr{B}\,| \prod_{i=l+1}^{n} m_i}_{④}. \tag{29}$$

We perform a similar investigation (as before) to determine which of the terms ①, ② and ④ of the inequality (29) is the dominant term. In Case (i), we find $④/① \le 2^{(n/2)+1}$, which means that $④ \le 2^{(n/2)+1}①$. And in Case (ii), we find $④/② \le 2^{n/2}/p$, which gives us that $④ \le 2^{n/2}/p②$. Hence for any *l*, we have

$$④ \le \left(2^{(n/2)+1}① + \frac{2^{n/2}}{p}② \right)$$

or

$$2^{n-l}\, p^{l-(n/2)-1} |\,\mathscr{B}\,| \prod_{i=l+1}^{n} m_i \le \left(2^{(n/2)+1} \frac{|\,\mathscr{B}\,|^2}{p^2} + \frac{2^{n/2}}{p}\, p^n |\,\mathscr{B}\,| \right).$$

Now looking at (29), we deduce

$$\sum_{\mathbf{x}\in V_{p^2}} \alpha(\mathbf{x}) \le (1 + 2^{(n/2)+1}) \frac{|\,\mathscr{B}\,|^2}{p^2} + \left(1 + \frac{2^{n/2}}{p} \right) p^n |\,\mathscr{B}\,|$$

$$\le \vartheta_n'' \left(\frac{|\,\mathscr{B}\,|^2}{p^2} + p^n |\,\mathscr{B}\,| \right), \tag{30}$$

where $\vartheta_n'' = 1 + 2^{(n/2)+1}$. Thus by (28),

$$|\,\mathscr{B} \cap V_{p^2}\,| \le \frac{2^n}{|\,\mathscr{B}\,|} \sum_{\mathbf{x}\in V_{p^2}} \alpha(\mathbf{x}) \le \vartheta_n'' 2^n \left(\frac{|\,\mathscr{B}\,|}{p^2} + p^n \right).$$

Lastly letting $\vartheta_n = 2^n \vartheta'_n$ if $\Delta = -1$ and $\vartheta_n = \vartheta''_n$ if $\Delta = +1$ we get from (27) and (30) that for $\Delta = \pm 1$, we have

$$|\mathscr{B} \cap V_{p^2}| \le \vartheta_n \left(\frac{|\mathscr{B}|}{p^2} + p^n \right).$$

This achieves the proof of the lemma. □

Lemma 4 is stated for boxes centered at the origin. In the next lemma we will drop this hypothesis and prove the lemma for arbitrary boxes.

Lemma 5. *Let p be an odd prime, $V_{p^2} = V_{p^2}(Q)$ be the set of zeros of* (2) *in $\mathbb{Z}^n_{p^2}$, and $\mathscr{B}$ be any box as given in* (1) *with all $m_i \le p^2$. If $\Delta_p = \pm 1$, then*

$$|\mathscr{B} \cap V_{p^2}| \le \gamma_n \left(\frac{|\mathscr{B}|}{p^2} + p^n \right),$$

where

$$\gamma_n = 2^n (1 + 6^n).$$

Proof. The fundamental identity $(\mathrm{mod}\ p^2)$ is

$$\sum_{\mathbf{x} \in V_{p^2}} \alpha(\mathbf{x}) = p^{-2} \sum_{\mathbf{x}} \alpha(\mathbf{x}) + p^n \underbrace{\sum_{\substack{y_i=1 \\ p^2 \mid Q^*(\mathbf{y})}}^{p^2} a(\mathbf{y})}_{E_0} - p^{n-1} \underbrace{\sum_{\substack{y_i=1 \\ p \mid Q^*(\mathbf{y})}}^{p^2} a(\mathbf{y})}_{E_1}$$

$$\underbrace{- \Delta p^{(3n/2)-2} \sum_{y'_i=1}^{p} a(p\mathbf{y}')}_{E_2} + \underbrace{\Delta p^{(3n/2)-1} \sum_{\substack{y'_i=1 \\ p \mid Q^*(\mathbf{y}')}}^{p} a(p\mathbf{y}')}_{E_3}.$$

Let $\alpha(\mathbf{x}) = \chi_{\mathscr{B}} * \chi_{\mathscr{B}'}$, where $\mathscr{B}' = \mathscr{B} - \mathbf{c}$. The value $\mathbf{c}$ is chosen such that $\mathscr{B}'$ is "nearly" centered at the origin:

$$c_i = a_i + \left[\frac{m_i - 1}{2} \right].$$

Then

$$\sum_{\mathbf{x}} \alpha(\mathbf{x}) = |\mathscr{B}||\mathscr{B}'| = |\mathscr{B}|^2,$$

$$\alpha(\mathbf{0}) = \sum_{\substack{u\in\mathscr{B} \\ \mathbf{u}+\mathbf{v}=\mathbf{0}}} \sum_{v\in\mathscr{B}'} 1 \le |\mathscr{B}|,$$

$$a(\mathbf{y}) = p^{2n} a_{\mathscr{B}}(\mathbf{y}) a_{\mathscr{B}'}(\mathbf{y}).$$

By using the Cauchy-Schwartz inequality (see [8]) and Parseval's identity (14), we get

$$\begin{aligned}
\sum_{\mathbf{y}} |a(\mathbf{y})| &= p^n \sum_{\mathbf{y}} |a_{\mathscr{B}}(\mathbf{y}) a_{\mathscr{B}'}(\mathbf{y})| \\
&\le p^n \left(\sum_{\mathbf{y}} |a_{\mathscr{B}}(\mathbf{y})|^2 \right)^{1/2} \left(\sum_{\mathbf{y}'} |a_{\mathscr{B}'}(\mathbf{y}')|^2 \right)^{1/2} \\
&\le p^n \left(\frac{1}{p^n} \sum_{\mathbf{y}} \chi^2_{\mathscr{B}}(\mathbf{x}) \right)^{1/2} \left(\frac{1}{p^n} \sum_{\mathbf{y}} \chi^2_{\mathscr{B}'}(\mathbf{x}) \right)^{1/2} \\
&= |\mathscr{B}|^{1/2} |\mathscr{B}'|^{1/2} = |\mathscr{B}|.
\end{aligned}$$

Then

$$|E_0 - E_1| = \left| p^n \sum_{\substack{y_i=1 \\ p^2 | Q^*(\mathbf{y})}}^{p^2} a(\mathbf{y}) - p^{n-1} \sum_{\substack{y_i=1 \\ p | Q^*(\mathbf{y})}}^{p^2} a(\mathbf{y}) \right| = \left| \sum_{y_i=1}^{p^2} \psi(\mathbf{y}) a(\mathbf{y}) \right|, \qquad (31)$$

where

$$\psi(\mathbf{y}) = \begin{cases} p^n - p^{n-1}, & p^2 | Q^*(\mathbf{y}), \\ -p^{n-1}, & p || Q^*(\mathbf{y}). \end{cases}$$

Continuing from (31),

$$|E_0 - E_1| \le (p^n - p^{n-1}) \sum_{\mathbf{y}} |a(\mathbf{y})| \le (p^n - p^{n-1}) |\mathscr{B}|.$$

Also,

$$|E_2 - E_3| = \left| -\Delta p^{(3n/2)-2} \sum_{y_i'=1}^{p} a(p\mathbf{y}') + \Delta p^{(3n/2)-1} \sum_{\substack{y_i'=1 \\ p \mid Q^*(\mathbf{y}')}}^{p} a(p\mathbf{y}') \right|$$

$$\leq \left| \sum_{y_i'=1}^{p} \theta(\mathbf{y}') a(p\mathbf{y}') \right|, \tag{32}$$

where

$$\theta(\mathbf{y}) = \begin{cases} p^{(3n/2)-1} - p^{(3n/2)-2}, & p \mid Q^*(\mathbf{y}), \\ p^{(3n/2)-2}, & p \nmid Q^*(\mathbf{y}). \end{cases}$$

Continuing from (32),

$$|E_2 - E_3| \leq (p^{3n/2-1} - p^{3n/2-2}) \sum_{y_i'=1}^{p} |a(p\mathbf{y}')|. \tag{33}$$

To complete the proof of Lemma 5, we need the following:

Lemma 6.

$$\sum_{|y_i| < p/2} |a_i(py_i)| \leq \begin{cases} 6\dfrac{m_i}{p} & \text{if } m_i \leq p, \\ 3\dfrac{m_i^2}{p^2} & \text{if } m_i > p. \end{cases}$$

Proof. We begin by establishing the inequality

$$\sum_{|y_i| > p/2m_i} \frac{1}{4y_i^2} \leq \begin{cases} 4\dfrac{m_i}{p} & \text{if } m_i \leq p/2, \\ 1 & \text{if } m_i > p/2. \end{cases} \tag{34}$$

We split the proof into two cases.

Case (I). If $\dfrac{p}{2m_i} \geq 1$, then

$$L = \left[\frac{p}{2m_i} \right] \geq \frac{1}{2} \frac{p}{2m_i} = \frac{p}{4m_i}.$$

Now

$$\sum_{y=L}^{\infty}\frac{1}{4y^2}=\frac{1}{4}\sum_{y=L}^{\infty}\frac{1}{y^2}\le\frac{1}{4L^2}+\frac{1}{4}\int_L^{\infty}\frac{dx}{x^2}$$

$$=\frac{1}{4L^2}+\frac{1}{4L}=\frac{1}{4L}\left(1+\frac{1}{L}\right)$$

$$\le\frac{2}{4L}=\frac{1}{2L}\le\frac{4m_i}{2p}=2\frac{m_i}{p}.$$

So

$$\sum_{|\,y_i\,|>p/2m_i}\frac{1}{4y_i^2}\le 4\frac{m_i}{p}.$$

Case (II). If $\frac{p}{2m_i}<1$, then by (19),

$$\sum_{|\,y_i\,|>p/2m_i}\frac{1}{4y_i^2}\le\frac{2}{4}\sum_{y=1}^{\infty}\frac{1}{y^2}\le\frac{\pi^2}{3\cdot 4}=\frac{\pi^2}{12}\le 1.$$

By Case (I) and Case (II), (34) follows.

We return to the proof of the lemma. Say $a(\mathbf{y})=\prod_{i=1}^{n}a_i(y_i)$. Then by the Fourier coefficients $a(\mathbf{y})=p^{2n}a_{\mathscr{B}}(\mathbf{y})a_{\mathscr{B}'}(\mathbf{y})$,

$$|\,a_i(y_i)\,|=p^2|\,a_{\mathscr{B},i}(y_i)a_{\mathscr{B}',i}(y_i)\,|=\frac{1}{p^2}\frac{\sin^2(\pi m_i y_i/p^2)}{\sin^2(\pi y_i/p^2)},$$

and so

$$|\,a_i(py_i)\,|\le\min\left\{\frac{m_i^2}{p^2},\frac{1}{4y_i^2}\right\},\quad\text{for}\quad|\,y_i\,|<p/2.$$

We consider four cases:

Case (i). If $m_i\le\frac{p}{2}$, then

$$\sum_{|\,y_i\,|<p/2}|\,a_i(py_i)\,|\le\sum_{|\,y_i\,|\le p/2m_i}\frac{m_i^2}{p^2}+\sum_{|\,y_i\,|>p/2m_i}\frac{1}{4y_i^2}$$

$$\le\frac{m_i^2}{p^2}\left(\frac{p}{m_i}+1\right)+\frac{4m_i}{p}=\frac{5m_i}{p}+\frac{m_i^2}{p^2}\le 6\frac{m_i}{p}.$$

Case (ii). If $m_i > \frac{p}{2}$, then

$$\sum_{|y_i|<p/2} |a_i(py_i)| \le \sum_{|y_i|\le p/2m_i} \frac{m_i^2}{p^2} + \sum_{|y_i|>p/2m_i} \frac{1}{4y_i^2}$$

$$\le \frac{m_i^2}{p^2}\left(\frac{p}{m_i}+1\right)+1 = \frac{m_i}{p}+\frac{m_i^2}{p^2}+1.$$

Case (iii). If $\frac{p}{2} < m_i < p$, then

$$\sum_{|y_i|<p/2} |a_i(py_i)| \le \frac{m_i}{p}+\frac{m_i^2}{p^2}+1 \le 2\frac{m_i}{p}+1 \le 4\frac{m_i}{p}.$$

Case (iv). If $m_i > p$, then

$$\sum_{|y_i|<p/2} |a_i(py_i)| \le 2\left(\frac{m_i}{p}\right)^2+1 \le 3\frac{m_i^2}{p^2},$$

completing the proof of Lemma 6. □

Proof of Lemma 5 (Continued). Suppose

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

By Lemma 6,

$$\sum_{|\mathbf{y}|<p/2} |a_i(p\mathbf{y})| = \prod_{i=1}^{n} \sum_{|y_i|<p/2} |a_i(py_i)| = \prod_{m_i\le p} 6\frac{m_i}{p} \prod_{m_i>p} 3\frac{m_i^2}{p^2}$$

$$\le 3^n 2^l \frac{|\mathscr{B}|}{p^n} \prod_{m_i>p} \frac{m_i}{p} = 3^n 2^l \frac{|\mathscr{B}|}{p^n} \frac{\prod_{m_i>p} m_i}{p^{n-l}}. \tag{35}$$

Using (35), then continuing from (33),

$$|E_2 - E_3| \le p^{(3n/2)-2}(p-1)\cdot 3^n 2^l p^{l-2n} |\mathscr{B}| \prod_{i=l+1}^{n} m_i.$$

Thus for $\Delta = \pm 1,$ the fundamental identity gives

$$\sum_{\mathbf{x}\in V_{p^2}} \alpha(\mathbf{x}) \le \frac{|\mathscr{B}|^2}{p^2} + |E_0 - E_1| + |E_2 - E_3|$$

$$\le \frac{|\mathscr{B}|}{p^2} + (p^n - p^{n-1})|\mathscr{B}| + p^{(3n/2)-2}(p-1)\cdot 3^n 2^l p^{l-2n}|\mathscr{B}|\prod_{i=l+1}^{n} m_i$$

$$\le \underbrace{\frac{|\mathscr{B}|^2}{p^2}}_{①} + \underbrace{p^n|\mathscr{B}|}_{②} + \underbrace{3^n 2^l p^{l-(n/2)-1}|\mathscr{B}|\prod_{i=l+1}^{n} m_i}_{❸}. \tag{36}$$

The task now is to determine which of the terms ①, ② and ❸ in (36) is the dominant term. We consider two cases:

Case (i). Suppose $l \le \frac{n}{2} - 1.$ Then compare

$$\frac{❸}{①} = \frac{3^n 2^l p^{l-(n/2)-1}|\mathscr{B}|\prod_{i=l+1}^{n} m_i}{|\mathscr{B}|^2/p^2}$$

$$= \frac{1}{|\mathscr{B}|} p^{l-(n/2)+1} 3^n 2^l \prod_{i=l+1}^{n} m_i$$

$$= \frac{p^{l-(n/2)+1} 3^n 2^l}{\prod_{i=1}^{l} m_i} \le 3^n 2^l p^{l-(n/2)+1} = 3^n 2^l.$$

This leads to

$$❸ \le 3^n 2^l \ ①.$$

Case (ii). Suppose $l \ge \frac{n}{2}.$ Then compare

$$\frac{❸}{②} = \frac{3^n 2^l p^{l-(n/2)-1}|\mathscr{B}|\prod_{i=l+1}^{n} m_i}{p^n|\mathscr{B}|} = 3^n 2^l p^{l-(3n/2)-1}\prod_{i=l+1}^{n} m_i$$

$$\leq 3^n 2^l p^{l-(3n/2)-1} p^{2(n-l)} = 3^n 2^l p^{(n/2)-1-l} \leq \frac{3^n 2^l}{p}.$$

This gives that

$$❸ \leq \frac{3^n 2^l}{p} ②.$$

So for any l, we have

$$❸ \leq \left(3^n 2^l ① + \frac{3^n 2^l}{p} ② \right).$$

Returning to (36), we now write

$$\begin{aligned} \sum_{\mathbf{x} \in V_{p^2}} \alpha(\mathbf{x}) &\leq ① + ② + ❸ \\ &\leq ① + ② + 3^n 2^l ① + \frac{3^n 2^l}{p} ② \\ &= (1 + 3^n 2^l)① + \left(1 + \frac{3^n 2^l}{p}\right)② \\ &\leq \gamma'_n \left(\frac{|\mathscr{B}|^2}{p^2} + p^n |\mathscr{B}| \right), \end{aligned} \tag{37}$$

where $\gamma'_n = 1 + 3^n 2^l$. On the other hand, it is easy to see that

$$\sum_{\mathbf{x} \in V_{p^2}} \alpha(\mathbf{x}) \geq \frac{1}{2^n} |\mathscr{B}| \, | V_{p^2} \cap \mathscr{B} |. \tag{38}$$

Hence it follows by combining (37) and (38) that

$$| \mathscr{B} \cap V_{p^2} | \leq 2^n \gamma'_n \left(\frac{|\mathscr{B}|}{p^2} + p^n \right) \leq \gamma_n \left(\frac{|\mathscr{B}|}{p^2} + p^n \right),$$

where $\gamma_n = 2^n (1 + 6^n)$. Lemma 5 is proved. □

Now, we prove Theorem 1.

Proof of Theorem 1. Partition $\mathscr{B}$ into $N = N_{\mathscr{B}}$ smaller boxes B_i,

$$\mathscr{B} = B_1 \cup B_2 \cup \cdots \cup B_N,$$

where each B_i has all of its edge lengths $\leq p^2$. Then we can apply Lemma 5 to each B_i, to get

$$\begin{aligned} |\, \mathscr{B} \cap V_{p^2,\mathbb{Z}} \,| &= \sum_{i=1}^{N} |\, B_i \cap V_{p^2} \,| \\ &\leq \sum_{i=1}^{N} \gamma_n \left(\frac{|\, B_i \,|}{p^2} + p^n \right) \\ &= \frac{\gamma_n}{p^2} \sum_{i=1}^{N} |\, B_i \,| + N\gamma_n p^n \\ &= \gamma_n \left(\frac{|\, \mathscr{B} \,|}{p^2} + N_{\mathscr{B}} p^n \right). \end{aligned}$$

The proof of Theorem 1 is complete. □

References

[1] T. Cochrane, Small solutions of congruences, Ph.D. Thesis, University of Michigan, 1984.

[2] A. Hakami, Small zeros of quadratic congruences to a prime power modulus, Ph.D. Thesis, Kansas State University, 2009.

[3] Ali H. Hakami, Small zeros of quadratic forms modulo p^2, JP J. Algebra Number Theory Appl. 17(2) (2010), 141-162.

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

[5] G. Myerson, The distribution of rational points on varieties defined over a finite field, Mathematika 28 (1981), 153-159.

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

[7] Myung-Hwan Kim et al., International Conference on Integral Forms and Lattices, Integral quadratic forms and lattices, Proceedings of the International Conference on Integral Quadratic Forms and Lattices, June 15-19, 1998, Seoul National University, Korea.

[8] H. L. King, Introduction to Number Theory, Springer-Verlag, 1982.