TAMKANG JOURNAL OF MATHEMATICS
Volume 46, Number 3, 349-364, September 2015
doi:10.5556/j.tkjm.46.2015.1745
This paper is available online at http://journals.math.tku.edu.tw/index.php/TKJM/pages/view/onlinefirst

PRIMITIVE ZEROS OF QUADRATIC FORMS MOD P^2

ALI H. HAKAMI

Abstract. Let $Q(\mathbf{x}) = Q(x_1, x_2, \ldots, x_n)$ be a quadratic form with integer coefficients, p be an odd prime and $\|\mathbf{x}\| = \max_i |x_i|$. A solution of the congruence $Q(\mathbf{x}) \equiv \mathbf{0} \pmod{p^2}$ is said to be a primitive solution if $p \nmid x_i$ for some i. In this paper, we seek to obtain primitive solutions of this congruence in small rectangular boxes of the type $\mathscr{B} = \{\mathbf{x} \in \mathbb{Z}^n : |x_i| \leq M_i,\ 1 \leqslant i \leqslant n\}$ where for $1 \leq i \leq l$ we have $M_i \leq p$, while for $i > l$ we have $M_i > p$. In particular, we show that if $n \geq 4$, n even, $l \leq \frac{n}{2} - 2$, and Q is nonsingular $\pmod{p}$, then there exists a primitive solution with $x_i = 0$, $1 \leq i \leq l$, and $|x_i| \leq 2^{\frac{4n+3}{n-l}} p^{\frac{n}{n-l}} + 1$, for $l < i \leq n$.

1. Introduction

Let $Q(\mathbf{x}) = Q(x_1, x_2, \ldots, x_n)$ be a quadratic form with integer coefficients and p be an odd prime. Set $\|\mathbf{x}\| = \max |x_i|$. When n is even we let $\Delta_p(Q) = \big((-1)^{n/2} \det A_Q / p\big)$ if $p \nmid \det A_Q$ and $\Delta_p(Q) = 0$ if $p | \det A_Q$, where $(\cdot/p)$ denotes the Legendre-Jacobi symbol and A_Q is the $n \times n$ defining matrix for $Q(\mathbf{x})$. $Q(\mathbf{x})$ is called nonsingular $\pmod{p}$ if $p \nmid \det A_Q$.

Consider the congruence

$$Q(\mathbf{x}) = Q(x_1, x_2, \ldots, x_n) \equiv 0 \pmod{m}, \tag{1}$$

where m is a positive integer. There has been much interest in obtaining a small nonzero solution of the congruence (1). The problem of finding a small solution of (1) means finding a nonzero integral solution $\mathbf{x}$ such that $\|\mathbf{x}\| \leq m^{\delta}$ for some positive constant $\delta < 1$. The constant δ may depend on n, but not on m.

In this paper we are seeking to find primitive solutions of (1) in a more general box centered at the origin, in the case where $m = p^2$. A primitive solution is one with $\gcd(x_1, \ldots, x_n, m) = 1$. A primitive solution is sought to rule out trivial solutions of (1) of the type $p\mathbf{y}$ where $\mathbf{y}$ satisfies $Q(\mathbf{y}) \equiv 0 \pmod{p}$. First, we give some background on what is already known for the case of small solutions.

Received September 21 , 2014, accepted March 17, 2015.
2010 *Mathematics Subject Classification*. Primary 11D79, 11E08, 11H50, 11H55.
Key words and phrases. Quadratic forms, congruences, small solutions.

For the quadratic form $Q(x) = x_1^2 + \cdots + x_n^2$, it is clear that any nonzero solution $\mathbf{x}$ of (1) must satisfy, $\max|x_i| \geq \frac{1}{\sqrt{n}} m^{1/2}$. Thus $\delta = 1/2$ is the best possible exponent for a small solution in general.

Schinzel, Schlickewei and Schmidt [17] proved that (1) has a nonzero solution with $\|\mathbf{x}\| < m^{(1/2)+1/2(n-1)}$ for $n \geq 2$, even, and $\|\mathbf{x}\| < m^{(1/2)+(1/2n)}$ for $n \geq 2$, odd. Thus for any $\varepsilon > 0$ we get a nonzero solution of (1) with $\|\mathbf{x}\| < m^{(1/2)+\varepsilon}$ provided n is sufficiently large. We note that the solution obtained by their method is not necessarily a primitive solution. Indeed, when $m = p^2$ they would simply use a trivial solution such as $(p, 0, \ldots, 0)$.

Dealing with $m = p$, p an odd prime, Heath-Brown [15] obtained a nonzero solution of (1) with $\|\mathbf{x}\| \ll p^{1/2} \log p$ for $n \geq 4$. His result was an improvement on the result of [17] in this case. Wang Yuan [18], [19] and [20] generalized Heath-Brown's work to all finite fields. Cochrane, in a sequence of papers [1], [2] and [3] improved this to $\|\mathbf{x}\| < \max\{2^{19} p^{1/2}, 2^{22} 10^6\}$. The best constant available is due to the author [7, Theorem 1.3] and [11, Theorem 1] who obtained $\|\mathbf{x}\| < \min\{p^{2/3}, 2^{19} p^{1/2}\}$.

Using the method of exponential sums the author [8, Theorem 1] generalized Cochrane's method to find a primitive solution of (1) with $\|\mathbf{x}\| \ll p$ for $n \geqslant 4$ when $m = p^2$ and $Q(\mathbf{y})$ is nonsingular $\pmod{p}$. The optimal bound, $\|x\| \leqslant p$ for $n \geqslant 1$, was obtained by Cochrane and Hakami using a geometric method [6, Theorem 1].

For $m = p^3$, the author [9, Theorem 1]. obtained the existence of a primitive solution of any nonsingular form with $\|\mathbf{x}\| \ll p^{(3/2)+(3/n)}$, provided $n \geqslant 6$.

For a general prime power $m = p^k$ and nonsingular form $\pmod{p^k}$ in $n \geqslant 4$ variables (n even) a primitive solution of size $\|\mathbf{x}\| \ll m^{(1/2)+(1/n)}$ is obtained by the author [10, Theorem 1].

For $m = pq$ a product of two distinct primes, the optimal bound, $\|\mathbf{x}\| \ll m^{1/2}$ for $n > 4$ was obtained by Cochrane [4] and [5], building upon the work of Heath-Brown [14]. But no attempt was made to obtain a primitive solution in this work.

As we mentioned our interest in this paper is the case $m = p^2$ with p a prime. We wish to obtain the existence of primitive solutions of the congruence

$$Q(\mathbf{x}) = Q(x_1, x_2, \ldots, x_n) \equiv 0 \pmod{p^2}, \tag{2}$$

in a box of points of the type

$$\mathscr{B} = \{\mathbf{x} \in \mathbb{Z}^n : |x_i| \leq M_i, \quad 1 \leq i \leq n\}, \tag{3}$$

centered about the origin, where $M_i \in \mathbb{Z}$, and $0 \leqslant M_i \leqslant \frac{p^2-1}{2}$ for $1 \leqslant i \leqslant n$. We shall assume that exactly l of the edges are of length at most p, while the remaining edges all have lengths strictly greater than p, say

$$2M_i + 1 \leq p, \quad 1 \leq i \leq l, \qquad 2M_i + 1 > p, \quad l + 1 \leq i \leq n.$$

We also restrict our attention to the case where n is even and Q is nonsingular $\pmod p$, so that $\Delta_p(Q)$ is as defined in the opening paragraph.

For the case $\Delta_p(Q) = 1$, we establish in Corollary 1 that if n is even, $n \geq 4$,

$$|\mathscr{B}| \geqslant 2^{4n+2} p^n, \quad \text{and} \quad \prod_{i=1}^{l} \frac{p}{2M_i + 1} \leqslant 2^{-4n-2} p^{(n/2)-1},$$

(where the product is set equal to 1 if $l = 0$), then there exists a primitive solution of (2) in the box $\mathscr{B} + \mathscr{B}$, that is, a primitive solution with $|x_i| \leq 2M_i$, $1 \leq i \leq n$. A similar result (where $4n+2$ is replaced by $4n+3$) is established in Corollary 2 for the case $\Delta_p(Q) = -1$. In the case where the first l edges are all of length zero, we deduce the following theorem.

Theorem 1. *Let p be an odd prime, Q be a quadratic form over $\mathbb{Z}$ in $n \geq 4$ variables with n even, and Q nonsingular $\pmod p$, and let l be a nonnegative integer with $l \leq \frac{n}{2} - 2$. Suppose that $p \geq 2^{\frac{2(n+3)}{n-2l-2}}$. Then there exists a primitive solution to (2) with $x_i = 0$, $1 \leq i \leq l$, and $|x_i| \leq 2^{\frac{4n+3}{n-l}} p^{\frac{n}{n-l}} + 1$, for $l < i \leq n$.*

In the case where $l = 0$, the theorem gives us a primitive solution of (2) with $\|\mathbf{x}\| \leq 2^{4+\frac{3}{n}} p$, recovering the type of bound obtained in [8] and [6]. To prove these results we shall use finite Fourier series over $\mathbb{Z}_{p^2}$, the modular ring in p^2 elements. The proof here builds upon the work of [6] and [8].

2. Basic identities and lemmas

In this section we shall assume that n is even, p is an odd prime, and that $Q(\mathbf{x})$ is a nonsingular quadratic form $\pmod p$ with $\Delta_p(Q) = \pm 1$. Let $e_{p^2}(\alpha) = e^{2\pi i \alpha / p^2}$. Let $V_{p^2} = V_{p^2}(Q)$ be the set of zeros of Q contained in $\mathbb{Z}_{p^2}^n$ and let $Q^*(\mathbf{y})$ be the quadratic form associated with inverse of the matrix for $Q \pmod p$. For $\mathbf{y} \in \mathbb{Z}_{p^2}^n$ set

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

We abbreviate complete sums over $\mathbb{Z}_{p^2}^n$ and $\mathbb{Z}_p^n$ in the manner

$$\sum_{\mathbf{x}} = \sum_{\mathbf{x} \bmod p^2} = \sum_{x_1=1}^{p^2} \cdots \sum_{x_n=1}^{p^2}, \qquad \sum_{\mathbf{x} \bmod p} = \sum_{x_1=1}^{p} \cdots \sum_{x_n=1}^{p}.$$

The following lemma gives us a formula for $\phi(V_{p^2}, \mathbf{y})$.

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

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

The proof of Lemma 1 is given (with some work) in Carlitz [14], and in complete detail in [13, Theorem 1].

Let $\alpha(\mathbf{x})$ be a complex valued function defined on $\mathbb{Z}^n_{p^2}$ with Fourier expansion $\alpha(\mathbf{x}) = \sum_{\mathbf{y}} a(\mathbf{y})e_{p^2}(\mathbf{x}\cdot\mathbf{y})$ where $a(\mathbf{y}) = p^{-2n}\sum_{\mathbf{x}}\alpha(\mathbf{x})e_{p^2}(-\mathbf{x}\cdot\mathbf{y})$. Then

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

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

$$\sum_{\mathbf{x}\in V}\alpha(\mathbf{x}) = p^{-2n}|V|\sum_{\mathbf{x}}\alpha(\mathbf{x}) + \sum_{\mathbf{y}\neq\mathbf{0}} a(\mathbf{y})\,\phi(V_{p^3},\mathbf{0}),\mathbf{y}).$$

Also by noticing that $|V| = \phi(V_{p^2},\mathbf{0}) + p^{2(n-1)}$, we obtain that

$$\sum_{\mathbf{x}\in V}\alpha(\mathbf{x}) = p^{-2}\sum_{\mathbf{x}}\alpha(\mathbf{x}) + \sum_{\mathbf{y}} a(\mathbf{y})\phi(V,\mathbf{y}). \tag{4}$$

Inserting the value of $\phi(V_{p^2},\mathbf{y})$ from Lemma 1 in (4) we obtain (see [8, Lemma 2])

Lemma 2 (The Fundamental Identity)**.** *Suppose n is even, Q is nonsingular* $\pmod p$ *and* $\Delta = \Delta_p(Q)$. *Then, for any complex valued $\alpha(\mathbf{x})$ on $\mathbb{Z}^n_{p^2}$,*

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

3. Proof of main results in the case where $\Delta_p(Q) = 1$

Let $\mathscr{B}$ be the box of points in $\mathbb{Z}^n$ given by

$$\mathscr{B} = \{\mathbf{x} \in \mathbb{Z}^n | a_i \le x_i < a_i + m_i, 1 \le i \le n\}, \tag{6}$$

where $m_i = q_i p + r_i$, $0 \leqslant r_i < p$ and $q_i, r_i \in \mathbb{Z}$. Thus the cardinality $\mathscr{B}$ is $|\mathscr{B}| = \prod_{i=1}^n m_i$. Consider the congruence

$$Q(\mathbf{x}) \equiv 0 \pmod{p}. \tag{7}$$

Our first step is to obtain an upper bound on the number of solutions of (7) contained in $\mathscr{B}$. First, we treat the case where all $m_i \leqslant p$. In this case we can view the box $\mathscr{B}$ in (6) as a subset of $\mathbb{Z}_p^n$ and appeal to the following result of Cochrane [1, Lemma 3].

Lemma 3. *Suppose that $\Delta_p(Q) = 1$. Let $\mathscr{B}$ be a box of type (6) with all $m_i \leqslant p$, and $V_p = V_p(Q)$ denote the set of zeros of (7) in $\mathbb{Z}_p^n$. Then*

$$\left|\mathscr{B} \cap V_p\right| \leqslant 2^n \left(\frac{|\mathscr{B}|}{p} + p^{n/2}\right). \tag{8}$$

Next we consider larger boxes where the m_i may exceed p. We define

$$N_{\mathscr{B}} = \prod_{i=1}^n \left(\left[\frac{m_i}{p}\right] + 1\right). \tag{9}$$

Partition the box $\mathscr{B}$ in (6) 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 $\leqslant p$. Thus Lemma 3 can be applied to each B_i. We obtain

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

Thus we have proved

Lemma 4. *Suppose that* $\Delta_p(Q) = 1$. *Let* $V_{p,\mathbb{Z}} = V_{p,\mathbb{Z}}(Q)$ *be the set of integer solutions of the congruence* (7). *Then for any box* $\mathscr{B}$ *of type* (6), *we have*

$$\left|\mathscr{B} \cap V_{p,\mathbb{Z}}\right| \leqslant 2^n \left(\frac{|\mathscr{B}|}{p} + N_{\mathscr{B}}\, p^{n/2}\right), \tag{10}$$

where $N_{\mathscr{B}}$ *as defined in* (9).

Let $\mathscr{B}$ be a box of points in $\mathbb{Z}^n$ as in (3) centered about the origin with edge lengths $m_i := 2M_i + 1 \leqslant p^2$, $1 \leq i \leq n$, and view this box as a subset of $\mathbb{Z}^n_{p^2}$. Let $\chi_{\mathscr{B}}$ be its characteristic function with 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 $\mathbf{y} \in \mathbb{Z}^n_{p^2}$,

$$a(\mathbf{y}) = p^{-2n} \prod_{i=1}^{n} \frac{\sin^2 \pi m_i y_i / p^2}{\sin^2 \pi y_i / p^2}, \tag{11}$$

where the term in the product is taken to be m_i if $y_i = 0$. In particular, if we take $\left|y_i\right| \leqslant p^2/2$ for all i, then using the fact that $|\sin(x)| \geqslant \frac{2}{\pi}|x|$ for $|x| \leqslant \pi/2$, we have

$$a(\mathbf{y}) \leqslant p^{-2n} \prod_{i=1}^{n} \min\left\{ m_i^2, \left(\frac{p^2}{2y_i}\right)^2 \right\}. \tag{12}$$

Since $\mathscr{B}$ is centered about the origin, the Fourier coefficients $a(\mathbf{y})$ are positive real numbers (as can be seen by (11)). Thus by applying the Fundamental Identity (5) to $\alpha(\mathbf{x}) = \chi_{\mathscr{B}} * \chi_{\mathscr{B}}$, we obtain

$$\begin{aligned}\sum_{\mathbf{x}\in V} \alpha(\mathbf{x}) &\geqslant \underbrace{p^{-2}\sum_{\mathbf{x}} \alpha(\mathbf{x})}_{\text{Main Term}} - \underbrace{p^{n-1} \sum_{p|Q^*(\mathbf{y})} a(\mathbf{y})}_{E_1} - \underbrace{p^{(3n/2)-2} \sum_{\mathbf{y} (\bmod p)} a(p\mathbf{y})}_{E_2} \\ &\geqslant \text{Main Term} - E_1 - E_2. \end{aligned} \tag{13}$$

The main term in (13) is

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

and the others are error terms. We proceed to bound these error terms.

First, we consider

$$E_1 = p^{n-1} \sum_{Q^*(\mathbf{y}) \equiv 0 \ (\bmod p)} a(\mathbf{y}). \tag{14}$$

Let $\sum^*$ be an abbreviation for $\sum_{Q^*(\mathbf{y})\equiv 0 (\bmod p), |y_i| < p^2/2}$. Define δ_i by

$$\delta_i = \begin{cases} 2^{k_i - 1} & \text{for } k_i \geq 1, \\ 0 & \text{for } k_i = 0. \end{cases} \tag{15}$$

Using (12) yields

$$\sum_{\substack{Q^*(\mathbf{y})\equiv 0 \pmod p\\ |y_i|\le p^2/2}} |a(\mathbf{y})| \le \sum_{k_1=0}^{\infty}\cdots\sum_{k_n=0}^{\infty} \sum^*_{\substack{\mathbf{y}\\ \delta_i \frac{p^2}{m_i}\le |y_i|\le 2^{k_i}\frac{p^2}{m_i}}} \prod_{i=1}^n \min\left\{\frac{m_i^2}{p^2}, \frac{p^2}{4y_i^2}\right\}$$

$$\le \sum_{k_1=0}^{\infty}\cdots\sum_{k_n=0}^{\infty} \sum^*_{\substack{\mathbf{y}\\ |y_i|\le 2^{k_i}\frac{p^2}{m_i}}} \prod_{i=1}^n \frac{p^2}{4(2^{k_i-1}p^2/m_i)^2}$$

$$= \frac{|\mathscr{B}|^2}{p^{2n}} \sum_{k_1=0}^{\infty}\cdots\sum_{k_n=0}^{\infty} \sum^*_{\substack{\mathbf{y}\\ |y_i|\le 2^{k_i}\frac{p^2}{m_i}}} \prod_{i=1}^n \frac{1}{2^{2k_i}}. \tag{16}$$

For non-negative integers $k_1, k_2, \ldots, k_n$, let

$$\mathscr{B}' = \left\{\mathbf{y}\in\mathbb{Z}_{p^2}^n : |y_i|\le 2^{k_i}\frac{p^2}{m_i},\ 1\le i\le n\right\}.$$

Put

$$m_i' = 2\left[\frac{2^{k_i}p^2}{m_i}\right]+1,$$

so that

$$|\mathscr{B}'| = \prod_{i=1}^n m_i' \le \prod_{i=1}^n \left(\frac{2^{k_i+1}p^2}{m_i}+1\right) \le \prod_{i=1}^n \frac{2^{k_i+2}p^2}{m_i} = 4^n\frac{p^{2n}}{|\mathscr{B}|}\prod_{i=1}^n 2^{k_i}. \tag{17}$$

Now, from the upper bound (10), we have

$$|\mathscr{B}'\cap V_{p,\mathbb{Z}}| \le 2^n\frac{|\mathscr{B}'|}{p} + 2^n N_{\mathscr{B}'}\, p^{n/2}, \tag{18}$$

where by utilizing (9),

$$N_{\mathscr{B}'} = \prod_{i=1}^n \left(\left[\frac{m_i'}{p}\right]+1\right) = \prod_{\substack{i=1\\ 2^{k_i}\ge \frac{m_i}{4p}}}^n \left(\left[\frac{m_i'}{p}\right]+1\right). \tag{19}$$

The last equality in (19) follows, since

$$2^{k_i} < \frac{m_i}{4p} \quad\Rightarrow\quad \frac{2^{k_i+1}p^2}{m_i}+1 < p \quad\Rightarrow\quad m_i' < p.$$

But the right-hand side of (19), is less than or equal to

$$\prod_{\substack{i=1\\ 2^{k_i}\ge \frac{m_i}{4p}}}^n \left(\frac{2^{k_i+1}p}{m_i}+\frac{1}{p}+1\right) \le 2^n \prod_{\substack{i=1\\ 2^{k_i}\ge \frac{m_i}{4p}}}^n \left(\frac{2^{k_i}p}{m_i}+1\right).$$

It follows that

$$N_{\mathscr{B}'} \leq 2^n \prod_{\substack{i=1 \\ 2^{k_i} \geq \frac{m_i}{4p}}}^{n} \left(\frac{2^{k_i} p}{m_i} + 1 \right). \tag{20}$$

Apply the upper bound (18) to the inner sum $\sum_{\mathbf{y}}^*$ in (16). This gives

$$\begin{aligned}
\sum_{\substack{Q^*(\mathbf{y}) \equiv 0 \pmod p \\ |y_i| \leq p^2/2}} a(\mathbf{y}) &= \frac{|\mathscr{B}|^2}{p^{2n}} \sum_{k_1=0}^{\infty} \cdots \sum_{k_n=0}^{\infty} \left| \mathscr{B}' \cap V_{p,\mathbb{Z}} \right| \prod_{i=1}^{n} \frac{1}{2^{2k_i}} \\
&\leq \frac{|\mathscr{B}|^2}{p^{2n}} \sum_{k_1=0}^{\infty} \cdots \sum_{k_n=0}^{\infty} \left(2^n \frac{|\mathscr{B}'|}{p} + 2^n N_{\mathscr{B}'} \, p^{n/2} \right) \prod_{i=1}^{n} \frac{1}{2^{2k_i}} \\
&= \sigma_1 + \sigma_2,
\end{aligned} \tag{21}$$

say. By employing the inequality (17), we find that

$$\begin{aligned}
\sigma_1 &= \frac{|\mathscr{B}|^2}{p^{2n}} \sum_{k_1=0}^{\infty} \cdots \sum_{k_n=0}^{\infty} \left(\prod_{i=1}^{n} \frac{1}{2^{2k_i}} \right) \frac{2^n |\mathscr{B}'|}{p} \\
&\leqslant \frac{|\mathscr{B}|^2}{p^{2n}} \sum_{k_1=0}^{\infty} \cdots \sum_{k_n=0}^{\infty} \left(\prod_{i=1}^{n} \frac{1}{2^{2k_i}} \right) \left(\frac{2^n}{p} 4^n \frac{p^{2n}}{|\mathscr{B}|} \prod_{i=1}^{n} 2^{k_i} \right) \\
&= 8^n \frac{|\mathscr{B}|}{p} \sum_{k_1=0}^{\infty} \cdots \sum_{k_n=0}^{\infty} \left(\prod_{i=1}^{n} \frac{1}{2^{k_i}} \right) \\
&\leqslant 8^n \cdot 2^n \frac{|\mathscr{B}|}{p} = 16^n \frac{|\mathscr{B}|}{p},
\end{aligned} \tag{22}$$

and by the inequality (21),

$$\begin{aligned}
\sigma_2 &= \frac{|\mathscr{B}|^2}{p^{2n}} \sum_{k_1=0}^{\infty} \cdots \sum_{k_n=0}^{\infty} 2^n N_{\mathscr{B}'} p^{n/2} \prod_{i=1}^{n} \frac{1}{2^{2k_i}} \\
&= 2^n \frac{|\mathscr{B}|^2}{p^{2n}} p^{n/2} \sum_{k_1=0}^{\infty} \cdots \sum_{k_n=0}^{\infty} 2^n \prod_{\substack{i=1 \\ 2^{k_i} \geq m_i/4p}}^{n} \left(\frac{2^{k_i} p}{m_i} + 1 \right) \prod_{i=1}^{n} \frac{1}{2^{2k_i}} \\
&= 4^n \frac{|\mathscr{B}|^2}{p^{2n}} p^{n/2} \prod_{i=1}^{n} \left[\sum_{\substack{k_i=0 \\ 2^{k_i} < m_i/4p}}^{\infty} \frac{1}{2^{2k_i}} + \sum_{\substack{k_i \\ 2^{k_i} \geqslant m_i/4p}} \left(\frac{2^{k_i} p}{m_i} + 1 \right) \frac{1}{2^{2k_i}} \right] \\
&\leq \frac{4^n |\mathscr{B}|^2}{p^{3n/2}} \prod_{i=1}^{n} \left[\sum_{k_i=0}^{\infty} \frac{1}{2^{2k_i}} + \sum_{\substack{k_i \\ 2^{k_i} \geq m_i/4p}} \frac{p}{2^{k_i} m_i} \right] \\
&= \frac{4^n |\mathscr{B}|^2}{p^{3n/2}} \prod_{i=1}^{n} \left[\frac{4}{3} + \frac{p}{m_i} \sum_{\substack{k_i=0 \\ 2^{k_i} \geqslant m_i/4p}}^{\infty} \frac{1}{2^{k_i}} \right]
\end{aligned}$$

$$\leq \frac{4^n|\mathscr{B}|^2}{p^{3n/2}}\prod_{i=1}^{n}\left[\frac{4}{3}+\min\left(\frac{2p}{m_i},\frac{8p^2}{m_i^2}\right)\right]. \tag{23}$$

Thus by (14), (21), (22) and (23), we have

$$\begin{aligned} E_1 &\leqslant 16^n\frac{|\mathscr{B}|}{p}p^{n-1}+\frac{4^n|\mathscr{B}|^2}{p^{3n/2}}p^{n-1}\prod_{i=1}^{n}\left[\frac{4}{3}+\min\left(\frac{2p}{m_i},\frac{8p^2}{m_i^2}\right)\right] \\ &= \underbrace{2^{4n}p^{n-2}|\mathscr{B}|}_{E_{1,1}}+\underbrace{\frac{4^n|\mathscr{B}|^2}{p^{n/2+1}}\prod_{i=1}^{n}\left[\frac{4}{3}+\min\left(\frac{2p}{m_i},\frac{8p^2}{m_i^2}\right)\right]}_{E_{1,2}}, \end{aligned} \tag{24}$$

where $E_{1,1}$, $E_{1,2}$ denote the terms underlined.

Let us now assume that for some positive integer l we have,

$$m_1 \leq \cdots \leq m_l \leq p < m_{l+1} \leq \cdots \leq m_n. \tag{25}$$

Then for $m_i \leq p$,

$$\frac{4}{3}+\min\left(\frac{2p}{m_i},8\left(\frac{p}{m_i}\right)^2\right) \leq \frac{4}{3}+\frac{2p}{m_i} \leq \frac{4p}{m_i}, \tag{26}$$

and for $m_i > p$,

$$\frac{4}{3}+\min\left(\frac{2p}{m_i},8\left(\frac{p}{m_i}\right)^2\right) \leq \frac{4}{3}+2 \leq \frac{10}{3}. \tag{27}$$

By (26) and (27), we can write

$$\prod_{i=1}^{n}\left[\frac{4}{3}+\min\left(\frac{2p}{m_i},\frac{8p^2}{m_i^2}\right)\right] \leq \prod_{i=1}^{l}\frac{4p}{m_i}\cdot\prod_{i=l+1}^{n}\frac{10}{3} = \frac{4^l p^l}{\prod_{i=1}^{l} m_i}\left(\frac{10}{3}\right)^{n-l} \leq \frac{4^n p^l}{\prod_{i=1}^{l} m_i}, \tag{28}$$

and consequently (using (23) and (28)),

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

Therefore, by inequalities (24) and (29), we arrive at

$$E_1 \leq \underbrace{2^{4n}p^{n-2}|\mathscr{B}|}_{E_{1,1}}+\underbrace{2^{4n}p^{l-(n/2)-1}|\mathscr{B}|\prod_{i=l+1}^{n} m_i}_{E_{1,2}}.$$

We next estimate the error term E_2, but to do that and also for future reference, we first prove

Lemma 5. *Let $\mathscr{B}$ be any box of type (3) and suppose that $\alpha(\mathbf{x}) = \chi_{\mathscr{B}} * \chi_{\mathscr{B}}(\mathbf{x})$, and that condition (25) holds. Then we have*

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

Proof. We first observe,

$$\begin{aligned}\sum_{y_i=1}^{p} a(p\mathbf{y}) &= \sum_{y_i=1}^{p}\sum_{x_i=\mathbf{1}}^{p^2}\frac{1}{p^{2n}}\alpha(\mathbf{x})e_{p^2}(-\mathbf{x}\cdot p\mathbf{y})\\ &= \sum_{x_i=1}^{p^2}\frac{1}{p^{2n}}\alpha(\mathbf{x})\sum_{y_i=1}^{p}e_p(-\mathbf{x}\cdot\mathbf{y})\\ &= \sum_{\substack{x_i=1\\ \mathbf{x}\equiv 0\,(\bmod p)}}^{p^2}\frac{p^n}{p^{2n}}\alpha(\mathbf{x})\\ &= \frac{1}{p^n}\sum_{\mathbf{x}\equiv 0\,(\bmod p)}\alpha(\mathbf{x})\\ &= \frac{1}{p^n}\sum_{\substack{\mathbf{u}\in\mathscr{B}\ \mathbf{v}\in\mathscr{B}\\ \mathbf{u}+\mathbf{v}\equiv 0\,(\bmod p)}} 1\\ &\le \frac{1}{p^n}\prod_{i=1}^{n} m_i\left(\left[\frac{m_i}{p}\right]+1\right). \end{aligned} \tag{30}$$

To obtain the last inequality in (30), we must count the number of solutions of the congruence

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

with $\mathbf{u},\mathbf{v}\in\mathscr{B}$. In fact 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 (25) then continuing from (30), we have

$$\begin{aligned}\sum_{y_i=1}^{p} a(p\mathbf{y}) &\le \frac{1}{p^n}\prod_{i=1}^{l} m_i \prod_{i=l+1}^{n} m_i\left(\frac{m_i}{p}+1\right)\\ &\le \frac{|\mathscr{B}|}{p^n}\prod_{i=l+1}^{n}\left(\frac{2m_i}{p}\right) \le \frac{2^{n-l}|\mathscr{B}|}{p^{2n-l}}\prod_{i=l+1}^{n} m_i.\end{aligned}$$

The lemma is established. □

Now in view of Lemma 5, it is clear that the error term E_2 has the estimate

$$E_2 = p^{(3n/2)-2}\sum_{\mathbf{y}(\bmod p)} a(p\mathbf{y}) \leqslant 2^{n-l}p^{l-(n/2)-2}|\mathscr{B}|\prod_{i=l+1}^{n} m_i.$$

The following theorem summarizes the final outcome of our investigation for the error terms

Theorem 2. *Suppose that $n \geq 4$, is even and that $\Delta_p(Q) = 1$, $V = V_{p^2}(Q)$. Then for any box $\mathscr{B}$ centered at the origin, with sides of length $m_i = 2M_i + 1$, $1 \leq i \leq n$, satisfying (25), we have*

$$\sum_{\mathbf{x}\in V} \alpha(\mathbf{x}) \geq \frac{|B|^2}{p^2} - |Error|,$$

where

$$|Error| \leq \underbrace{2^{4n} p^{n-2}|\mathscr{B}|}_{E_{1,1}} + \underbrace{2^{4n} p^{l-(n/2)-1}|\mathscr{B}| \prod_{i=l+1}^{n} m_i}_{E_{1,2}} + \underbrace{2^n p^{l-(n/2)-2}|\mathscr{B}| \prod_{i=l+1}^{n} m_i}_{E_2}.$$

In Theorem 2 we have indicated below each term, the error term bounded by the given value.

Next we compare each error term in Theorem 2 to the main term $|B|^2/p^2$. To make the left-hand side positive, we make each error term less than 1/4 of the main term. For the error term $E_{1,1}$, we need

$$\frac{1}{4}\frac{|\mathscr{B}|^2}{p^2} \geq 2^{4n} p^{n-2}|\mathscr{B}| \Longleftrightarrow |\mathscr{B}| \geq 2^{4n+2} p^n,$$

and for the error term $E_{1,2}$,

$$\frac{1}{4}\frac{|\mathscr{B}|^2}{p^2} \geq 2^{4n} p^{l-(n/2)-1}|\mathscr{B}| \prod_{i=l+1}^{n} m_i \Longleftrightarrow \prod_{i=1}^{l} m_i \geq 2^{4n+2} p^{l-(n/2)+1} \Longleftrightarrow \prod_{i=1}^{l} \frac{p}{m_i} \leq 2^{-4n-2} p^{(n/2)-1}.$$

Finally for the error term E_2,

$$\frac{1}{4}\frac{|\mathscr{B}|^2}{p^2} \geq 2^{n} p^{l-(n/2)-2}|\mathscr{B}| \prod_{i=l+1}^{n} m_i \Longleftrightarrow |\mathscr{B}| \geq 4\cdot 2^n p^{l-(n/2)} \prod_{i=l+1}^{n} m_i \Longleftrightarrow \prod_{i=1}^{l} \frac{p}{m_i} \leq 2^{-(n+2)} p^{(n/2)}.$$

Putting the pieces together, we deduce

Theorem 3. *Suppose that $n \geq 4$ is even, $\Delta_p(Q) = 1$ and that $V = V_{p^2}(Q)$. Let $\mathscr{B}$ be a box centered at the origin satisfying (25). If $|\mathscr{B}| \geqslant 2^{4n+2}p^n$ and $\prod_{i=1}^{l}(p/m_i) \leqslant 2^{-4n-2}p^{(n/2)-1}$ (where L.H.S = 1 if $l = 0$), then*

$$\sum_{\mathbf{x}\in V} \alpha(\mathbf{x}) \geq \frac{|\mathscr{B}|^2}{p^2} - \frac{3}{4}\frac{|\mathscr{B}|^2}{p^2} = \frac{1}{4}\frac{|\mathscr{B}|^2}{p^2}.$$

In particular,

$$|V \cap (\mathscr{B} + \mathscr{B})| \geq \frac{|\mathscr{B}|}{4p^2}.$$

Recall that a solution of (3) is called primitive if some coordinate is not divisible by p, i.e $p \nmid x_i$ for some i. We write $p|\mathbf{x}$ for imprimitive points.

Corollary 1. *Under the hypothesis of Theorem 3, $\mathscr{B} + \mathscr{B}$ contains a primitive solution of (2).*

Proof. We need to show that

$$\sum_{\mathbf{x}\in V} \alpha(\mathbf{x}) > \sum_{\substack{\mathbf{x}\in V\\ p|\mathbf{x}}} \alpha(\mathbf{x}).$$

First by Lemma 5,

$$\begin{aligned}\sum_{\substack{\mathbf{x}\in V\\ p|\mathbf{x}}} \alpha(\mathbf{x}) &= \sum_{\substack{p|x_i,\\ 1\le i\le n}} \alpha(\mathbf{x}) = p^n \sum_{y=1}^{p} a(p\mathbf{y}) \le 2^{n-l} p^{l-n} |\mathscr{B}| \prod_{i=l+1}^{n} m_i \\ &= \frac{1}{2^l}\cdot\frac{2^n|\mathscr{B}|}{p^{n-l}} \prod_{i=l+1}^{n} m_i \le \frac{1}{2^l}\cdot\frac{|\mathscr{B}|^2}{4p^2}.\end{aligned}$$

The last inequality is guaranteed by our hypothesis (Theorem 3) that

$$\prod_{i=1}^{l} \frac{p}{m_i} \le 2^{-4n-2} p^{(n/2)-1}. \tag{31}$$

More precisely, assume (31), then certainly

$$\prod_{i=1}^{l} \frac{p}{m_i} \le \frac{p^{(n/2)-1}}{2^{4n+2}} \quad\Rightarrow\quad \frac{2^n}{p^{n-l}} \prod_{i=l+1}^{n} m_i < \frac{|\mathscr{B}|}{4p^2}.$$

So we have now on the one hand,

$$\sum_{\substack{\mathbf{x}\in V\\ p|\mathbf{x}}} \alpha(\mathbf{x}) \;<\; \frac{|\mathscr{B}|^2}{4p^2}.$$

On the other hand, by Theorem 3, we have

$$\sum_{\mathbf{x}\in V} \alpha(\mathbf{x}) \;\ge\; \frac{|\mathscr{B}|^2}{4p^2}.$$

We therefore get

$$\sum_{\substack{\mathbf{x}\in V\\ p\nmid\mathbf{x}}} \alpha(\mathbf{x}) \;\geqslant \frac{|\mathscr{B}|^2}{4p^2} \;-\sum_{\substack{\mathbf{x}\in V\\ p|\mathbf{x}}} \alpha(\mathbf{x}) > 0.$$

The proof of the corollary is complete. □

4. Proof of Main Results in the case where $\Delta_p(Q) = -1$

Suppose now that n is even and that $\Delta_p(Q) = -1$. We first need to produce analogues of Lemmas 3 and 4 as follows; see [7, Lemma 2.9] and [12, Theorem 1].

Lemma 6. *Let $\mathscr{B}$ be any box of type (6) with all $m_i \leqslant p$, and $V_p = V_p(Q)$ denote to the set of solutions of (7) in $\mathbb{Z}_p^n$. Then*

$$\left|\mathscr{B}\cap V_p\right| \leqslant 2^{n+1}\left(\frac{|\mathscr{B}|}{p} + p^{n/2}\right).$$

Lemma 7. *Let $V_{p,\mathbb{Z}} = V_{p,\mathbb{Z}}(Q)$ be the set of integer solutions of the congruence (7). Then for any box of type (6),*

$$\left|\mathscr{B} \cap V_{p,\mathbb{Z}}\right| \leqslant 2^{n+1}\left(\frac{|\mathscr{B}|}{p} + N_{\mathscr{B}}\, p^{n/2}\right), \tag{32}$$

where $N_{\mathscr{B}}$ is given in (9).

Applying the Fundamental Identity (5) to $\alpha(\mathbf{x}) = \chi_{\mathscr{B}} * \chi_{\mathscr{B}}$ as in the preceding section, but this time with $\Delta = -1$, we have

$$\sum_{\mathbf{x}\in V} \alpha(\mathbf{x}) \geqslant \underbrace{p^{-2}\sum_{\mathbf{x}} \alpha(\mathbf{x})}_{\text{Main Term}} - \underbrace{p^{n-1} \sum_{p|Q^*(\mathbf{y})} a(\mathbf{y})}_{E_1} - \underbrace{p^{(3n/2)-1} \sum_{\substack{p|Q^*(\mathbf{y}') \\ \mathbf{y}' (\bmod p)}} a(p\mathbf{y}')}_{E_3}. \tag{33}$$

Next we seek bounds on the error terms in (33). For the error term E_1 we have already seen in the case $\Delta = 1$ how this error term is bounded. The same strategy will work in the case $\Delta = -1$, except we shall make use of the upper bound (32) in Lemma 7 instead of the upper bound (10) in Lemma 4. We find that

$$\begin{aligned}
\sum_{\substack{Q^*(\mathbf{y}) \equiv 0 (\bmod p) \\ |y_i| \leq p^2/2}} |a(\mathbf{y})| &= \frac{|\mathscr{B}|^2}{p^{2n}} \sum_{k_1=0}^{\infty} \cdots \sum_{k_n=0}^{\infty} |\mathscr{B}' \cap V_{\mathbb{Z}}| \prod_{i=1}^{n} \frac{1}{2^{2k_i}} \\
&\leqslant \frac{|\mathscr{B}|^2}{p^{2n}} \sum_{k_1=0}^{\infty} \cdots \sum_{k_n=0}^{\infty} \left(2^{n+1}\frac{|\mathscr{B}'|}{p} + 2^{n+1} N_{\mathscr{B}'}\, p^{n/2}\right) \prod_{i=1}^{n} \frac{1}{2^{2k_i}} \\
&\ \vdots \\
&\leqslant 2 \cdot 16^n \frac{|\mathscr{B}|}{p} + \frac{|\mathscr{B}|^2 4^n}{p^{3n/2}} \prod_{i=1}^{n} \left[\frac{4}{3} + \min\left(\frac{2p}{m_i}, \frac{8p^2}{m_i^2}\right)\right].
\end{aligned}$$

Thus, it follows that

$$E_1 \leqslant \underbrace{2^{4n+1} p^{n-2} |\mathscr{B}|}_{E_{1,1}} + \underbrace{\frac{2 \cdot 4^n |\mathscr{B}|^2}{p^{n/2+1}} \prod_{i=1}^{n} \left[\frac{4}{3} + \min\left(\frac{2p}{m_i}, \frac{8p^2}{m_i^2}\right)\right]}_{E_{1,2}}. \tag{34}$$

Assume (as before) that

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

Then for $m_i \leqslant p$,

$$\frac{4}{3} + \min\left(\frac{2p}{m_i}, 8\left(\frac{p}{m_i}\right)\right)^2 \leqslant \frac{4}{3} + \frac{2p}{m_i} \leqslant \frac{4p}{m_i},$$

and for $m_i > p$,

$$\frac{4}{3}+\min\left(\frac{2p}{m_i},8\left(\frac{p}{m_i}\right)^2\right)\leqslant\frac{4}{3}+2\leqslant\frac{10}{3}.$$

By taking account of these two inequalities, we have

$$\prod_{i=1}^{n}\left[\frac{4}{3}+\min\left(\frac{2p}{m_i},\frac{8p^2}{m_i^2}\right)\right]\leqslant\prod_{i=1}^{l}\frac{4p}{m_i}\cdot\prod_{i=l+1}^{n}\frac{10}{3}=\frac{4^l p^l}{\prod_{i=1}^{l}m_i}\left(\frac{10}{3}\right)^{n-l}\leqslant\frac{4^n p^l}{\prod_{i=1}^{l}m_i}. \tag{35}$$

Using (34) and (35), we infer that

$$E_{1,2}\leqslant\frac{2\cdot 4^n|\mathscr{B}|^2}{p^{n/2+1}}\frac{4^n p^l}{\prod_{i=1}^{l}m_i}=\frac{2^{4n+1}\prod_{i=1}^{n}m_i^2}{p^{n/2-l+1}\cdot\prod_{i=1}^{l}m_i}=2^{4n+1}p^{l-(n/2)-1}|\mathscr{B}|\prod_{i=l+1}^{n}m_i.$$

To estimate the error term E_3, we just need to apply Lemma 5. It is easily seen that

$$E_3=p^{(3n/2)-1}\sum_{\mathbf{y}(\text{ mod } p)}a(p\mathbf{y})\leqslant 2^{n-l}p^{l-(n/2)-1}|\mathscr{B}|\prod_{i=l+1}^{n}m_i. \tag{36}$$

Thus, we have established,

Theorem 4. *Suppose that $n\geqslant 4$ is even, $\Delta_p(Q)=-1$ and that $V=V_{p^2}(Q)$. Then for any box $\mathscr{B}$ centered at the origin,*

$$\sum_{\mathbf{x}\in V}\alpha(\mathbf{x})\geqslant\frac{|\mathscr{B}|^2}{p^2}-|Error|,$$

where

$$|Error|\leqslant\underbrace{2^{4n+1}p^{n-2}|\mathscr{B}|}_{E_{1,1}}+\underbrace{2^{4n+1}p^{l-(n/2)-1}|\mathscr{B}|\prod_{i=l+1}^{n}m_i}_{E_{1,2}}+\underbrace{2^{n}p^{l-(n/2)-1}|\mathscr{B}|\prod_{i=l+1}^{n}m_i}_{E_3}.$$

As before, in order to obtain a positive sum we seek conditions such that each error term is less than 1/4 of the main term.

$$E_{1,1}:\quad\frac{1}{4}\frac{|\mathscr{B}|^2}{p^2}\geqslant 2^{4n+1}p^{n-2}|\mathscr{B}|\Longleftrightarrow|\mathscr{B}|\geqslant 2^{4n+3}p^n.$$

$$E_{1,2}:\quad\frac{1}{4}\frac{|\mathscr{B}|^2}{p^2}\geqslant 2^{4n+1}p^{l-(n/2)-1}|\mathscr{B}|\prod_{i=l+1}^{n}m_i\Longleftrightarrow\prod_{i=1}^{l}\frac{p}{m_i}\leqslant 2^{-4n-3}p^{(n/2)-1}.$$

$$E_3:\quad\frac{1}{4}\frac{|\mathscr{B}|^2}{p^2}\geqslant 2^{n-l}p^{l-(n/2)-1}|\mathscr{B}|\prod_{i=l+1}^{n}m_i\Longleftrightarrow\prod_{i=1}^{l}\frac{p}{m_i}\leqslant 2^{l-n-2}p^{(n/2)-1}.$$

Thus we obtain,

Theorem 5. *Suppose that $n \geqslant 4$ is even, $\Delta_p(Q) = -1$ and that $V = V_{p^2}(Q)$. If $\mathscr{B}$ is a box satisfying* (25), $|\mathscr{B}| \geqslant 2^{4n+3}p^n$ *and* $\prod_{i=1}^{l}(p/m_i) \leqslant 2^{-4n-3}p^{(n/2)-1}$ *(with L.H.S = 1 if $l = 0$), then*

$$\sum_{\mathbf{x}\in V} \alpha(\mathbf{x}) \geqslant \frac{|\mathscr{B}|^2}{p^2} - \frac{3}{4}\frac{|\mathscr{B}|^2}{p^2} = \frac{1}{4}\frac{|\mathscr{B}|^2}{p^2}.$$

In particular,

$$|V \cap (\mathscr{B}+\mathscr{B})| \geqslant \frac{|\mathscr{B}|}{4p^2}.$$

As a consequence of Theorem 5, we have the following analogue of Corollary 1 for primitive solutions; the proof is identical to the proof of Corollary 1.

Corollary 2. *Under the hypotheses of Theorem 5, $\mathscr{B}+\mathscr{B}$ contains a primitive solution of* (2).

5. Proof of Theorem 1

Let p be an odd prime, Q be a quadratic form over $\mathbb{Z}$ in $n \geq 4$ variables with n even, and Q nonsingular $\pmod p$, and let l be a nonnegative integer with $l \leq \frac{n}{2} - 2$. Set $m_i = 2M_i + 1$, $1 \leq i \leq n$. For $0 \leq i \leq l$, set $M_i = 0$, while for $l < i \leq n$, set $M_i = \lceil 2^{\frac{4n+3}{n-l}-1} p^{\frac{n}{n-l}} - \frac{1}{2}\rceil$. Then for $1 \leq i \leq l$ we have $m_i = 1$, while for $l < i \leq n$ we have $m_i > 2^{\frac{4n+3}{n-l}} p^{\frac{n}{n-l}}$, and so

$$|\mathscr{B}| = \prod_{i=l+1}^{n} m_i > 2^{4n+3}p^n,$$

and

$$\prod_{i=1}^{l} \frac{p}{m_i} = p^l \leq 2^{-4n-3} p^{\frac{n}{2}-1},$$

for $p \geq 2^{\frac{2(n+3)}{n-2l-2}}$. Thus the hypotheses of both Corollary 1 and Corollary 2 are satisfied, and so there exists a primitive solution of the congruence $Q(\mathbf{x}) \equiv 0 \pmod{p^2}$ in the box $\mathscr{B}+\mathscr{B}$, that is a solution with $x_i = 0$, $1 \leq i \leq l$ and for $l < i \leq n$,

$$|x_i| \leq 2M_i = 2\lceil 2^{\frac{4n+3}{n-l}-1} p^{\frac{n}{n-l}} - \tfrac{1}{2}\rceil \leq 2^{\frac{4n+3}{n-l}} p^{\frac{n}{n-l}} + 1.$$

Acknowledgements

The authors would like to sincerely thank the anonymous referee for very valuable and helpful comments and suggestions which made the paper more accurate and readable.

References

[1] T. Cochrane, *Small zeros of quadratic forms modulo p*, J. Number Theory, **33**(1989), 286–292.

[2] T. Cochrane, *Small zeros of quadratic forms modulo p, II,* Proceedings of the Illinois Number Theory Conference, (1989), Birkhäuser, Boston (1990), 91–94.

[3] T. Cochrane, *Small zeros of quadratic forms modulo p, III,* J. Number Theory, **33** (1991), 92–99.

[4] T. Cochrane, *Small zeros of quadratic congruences modulo pq*, Mathematika, **37** (1990), 261–272.

[5] T. Cochrane, *Small zeros of quadratic congruences modulo pq, II,* J. Number Theory **50** (1995), 299–308.

[6] T. Cochrane and A. Hakami, *Small zeros of quadratic congruences modulo p^2,* Proceedings of the American Mathematical Society, **140** (2012), 4041–4052.

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

[8] A. Hakami, *Small zeros of quadratic forms modulo p^2,* JP J. Algebra, Number Theory and Applications, **17** (2011), 141–162.

[9] A. Hakami, *Small zeros of quadratic forms modulo p^3,* Advances and Applications in Mathematical Sciences, **9** (2011), 47–69.

[10] A. Hakami, *Small primitive zeros of quadratic forms modulo p^m,* The Ramanujan J (2014), DOI 10.1007/s11139–014–9614–3.

[11] A. Hakami, *On Cochrane's estimate for small zeros of quadratic forms modulo p,* Far East J. Math. Sciences, **50** (2011), 151–157.

[12] A. Hakami, *An upper bound for the number of integral solutions of quadratic forms modulo p,* J. Algebra, Number Theory: Advances and Applications, **6** (2011), 1–17.

[13] A. Hakami, *Weighted quadratic partitions $(mod\ p^m)$, A new formula and new demonstration,* Tamaking J. Math., **43** (2012), 11–19.

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

[15] D. R. Heath–Brown, *Small solutions of quadratic congruences,* Glasgow Math. J, **27** (1985), 87–93.

[16] D.R. Heath–Brown, *Small solutions of quadratic congruences II,* Mathematika, **38** (1991), 264–284.

[17] A. Schinzel, H.P. Schlickewei and W.M. Schmidt, *Small solutions of quadratic congruences and small fractional parts of quadratic forms,* Acta Arithmetica, **37** (1980), 241–248.

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

[19] Y. Wang, *On small zeros of quadratic forms over finite fields,* J. Number Theory, **31** (1989), 272–284.

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

Department of Mathematics, Jazan University, P.O.Box 277, Jazan, Postal Code: 45142, Saudi Arabia.

E-mail: aalhakami@jazanu.edu.sa