Hakami *Journal of Inequalities and Applications* (2015) 2015:110
DOI 10.1186/s13660-015-0637-0

Journal of Inequalities and Applications
a SpringerOpen Journal

RESEARCH Open Access

Estimates for lattice points of quadratic forms with integral coefficients modulo a prime number square (II)

Ali H Hakami*

*Correspondence: aalhakami@jazanu.edu.sa
Department of Mathematics, Jazan University, P.O. Box 277, Jazan, 45142, Saudi Arabia

Abstract

Let $Q(\mathbf{x}) = Q(x_1, x_2, \ldots, x_n)$ be a nonsingular quadratic form with integer coefficients, n be even and p be an odd prime. In Hakami (J. Inequal. Appl. 2014:290, 2014, doi:10.1186/1029-242X-2014-290) we obtained an upper bound on the number of integer solutions of the congruence $Q(\mathbf{x}) \equiv 0 \pmod{p^2}$ in small boxes of the type $\{\mathbf{x} \in \mathbb{Z}_{p^2}^n | a_i \le x_i < a_i + m_i, 1 \le i \le n\}$, centered about the origin, where $a_i, m_i \in \mathbb{Z}$, $0 < m_i \le p^2$, $1 \le i \le n$. In this paper, we shall drop the hypothesis of 'centered about the origin' and generalize the result of paper Hakami (J. Inequal. Appl. 2014:290, 2014, doi:10.1186/1029-242X-2014-290) to boxes of arbitrary size and position.

MSC: 11E04; 11E08; 11E12; 11P21

Keywords: Lattice theory; quadratic forms; lattice points; congruences

1 Introduction

Let $Q(\mathbf{x}) = Q(x_1, x_2, \ldots, x_n) = \sum_{1 \le i \le j \le n} a_{ij} x_i x_j$ be a quadratic form with integer coefficients in n-variables, p be an odd prime, $\mathbb{Z}_{p^2} = \mathbb{Z}/(p^2)$, and $V_{p^2} = V_{p^2}(Q)$ be the algebraic subset of $\mathbb{Z}_{p^2}^n$ defined by the equation

$$Q(\mathbf{x}) = Q(x_1, x_2, \ldots, x_n) = 0. \tag{1.1}$$

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 $(\cdot/p)$ denotes the Legendre-Jacobi symbol and A_Q is the $n \times n$ defining matrix for $Q(\mathbf{x})$. We call Q a nonsingular form $\pmod p$ if $p \nmid \det A_Q$. As usual, we let $|S|$ denote the cardinality of a set S.

Our first interest in this paper is obtaining an estimate for the number of solutions of (1.1) in a box of the type

$$\mathcal{B} = \left\{\mathbf{x} \in \mathbb{Z}^n | a_i \le x_i < a_i + m_i, 1 \le i \le n\right\}, \tag{1.2}$$

viewed as a subset of $\mathbb{Z}_{p^2}^n$, where $a_i, m_i \in \mathbb{Z}$, $0 < m_i \le p^2$, $1 \le i \le n$.

Theorem 1 *Suppose that n is even, Q is a nonsingular form* $\pmod p$ *and that $V_{p^2}(Q)$ is the set of solutions of* (1.1). *Then, for any box $\mathcal{B}$ of type* (1.2) (*viewed as a subset of $\mathbb{Z}_{p^2}^n$*) *with*

$0 < m_i \le p^2$, $1 \le i \le n$, *we have*

$$\left|\mathcal{B} \cap V_{p^2}(Q)\right| \le \gamma_n\left(\frac{|\mathcal{B}|}{p^2} + p^n\right), \tag{1.3}$$

where

$$\gamma_n = 2^n\left(1 + 6^n\right). \tag{1.4}$$

We conjecture that the following upper bound holds:

$$\left|\mathcal{B} \cap V_{p^2}(Q)\right| \le \frac{|\mathcal{B}|}{p^2} + O_\epsilon\left(p^{n-2+\epsilon}\right),$$

which would be the best possible estimate. Indeed, for the form $Q(\mathbf{x}) = x_1x_2 - x_3x_4$, the ϵ factor cannot be removed altogether. For this form it is known [1], Theorem 3, that the number of solutions of the equation $Q(\mathbf{x}) = 0$ in integers $\mathbf{x}$ with $1 \le x_i \le B$ is asymptotic to $\frac{12}{\pi^2}B^2 \log B$. Thus, for any B, the number of solutions of the congruence $Q(\mathbf{x}) \equiv 0 \pmod{p^2}$ with $1 \le x_i \le B$ is at least $\frac{12}{\pi^2}B^2 \log B$. Letting $B \approx p$ demonstrates the optimality of the conjectured upper bound. In Section 3 we establish the asymptotic estimate

$$\left|\mathcal{B} \cap V_{p^2}(Q)\right| = \frac{|\mathcal{B}|}{p^2} + O\left(p^{\frac{3}{2}n-1} \log^n p\right).$$

The error term p^n in the upper bound (1.3) greatly improves on the error term $p^{\frac{3}{2}n-1} \log^n p$ in the asymptotic estimate at the expense of having to place a constant larger than 1 on the main term. We would expect that the error term in the asymptotic estimate can be improved at least to the value p^n appearing in our upper bound.

In the next theorem the same type of bound as Theorem 1 is given for boxes with sides of unrestricted lengths. In this case, we let $V_{p^2,\mathbb{Z}}$ denote the set of integer solutions of the congruence

$$Q(\mathbf{x}) \equiv 0 \pmod{p^2}, \tag{1.5}$$

and regard $\mathcal{B}$ as a set of points in $\mathbb{Z}^n$.

Theorem 2 *Suppose that n is even, Q is nonsingular* $(\bmod\, p)$ *and $V_{p^2,\mathbb{Z}} = V_{p^2,\mathbb{Z}}(Q)$ is the set of integer solutions of the congruence* (1.5). *Then, for any box $\mathcal{B}$ of type* (1.2) (*allowing $m_i > p^2$*), *we have*

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

where γ_n is as in (1.4), *and*

$$N_{\mathcal{B}} = \prod_{i=1}^{n}\left\lceil \frac{m_i}{p^2} \right\rceil.$$

We devote Section 4 and Section 5 respectively to the proofs of Theorem 1 and Theorem 2.

2 Preliminary lemmas

For any $\mathbf{x}, \mathbf{y}$ in $\mathbb{Z}_{p^2}^n$, we 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. For $\mathbf{y} \in \mathbb{Z}_{p^2}^n$, we write $p|\mathbf{y}$ if $p|y_i$, $1 \le i \le n$ (where the y_i are regarded as integer representatives for the residue classes). In this case $\frac{1}{p}\mathbf{y}$ is a well-defined element of $\mathbb{Z}_{p^2}^n$. Let Q be a nonsingular quadratic form $(\operatorname{mod} p)$, and $V_{p^2} = V_{p^2}(Q)$ be the set of solutions of (1.1). For $\mathbf{y} \in \mathbf{Z}_{p^2}^n$ we define

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

The following lemma was established in [2].

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

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

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

In [3] we established the basic identity

$$\sum_{\mathbf{x}\in V_{p^2}} \alpha(\mathbf{x}) = p^{2n-2} a(\mathbf{0}) + \sum_{\mathbf{y}} a(\mathbf{y})\phi(V_{p^2}, \mathbf{y}) \tag{2.1}$$

for any complex valued function $\alpha(\mathbf{x})$ defined on $\mathbb{Z}_{p^2}$ with Fourier expansion

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

Inserting the value of $\phi(V_{p^2}, \mathbf{y})$ from Lemma 1 into the basic identity (2.1) yields the following (see [4]).

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

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

3 Asymptotic estimate of $|\mathcal{B} \cap V_{p^2}|$

To obtain an asymptotic estimate for the number of solutions of (1.5) in a box $\mathcal{B}$ with sides of length $m_i \le p^2$, we let $\alpha = \chi_{\mathcal{B}}$, the characteristic function for the box. For such α, it is well known that the Fourier coefficients $a_{\mathcal{B}}(\mathbf{y})$ have magnitude

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

where the term in the product is taken to be m_i if $y_i = 0$. Henceforth, we choose representatives $\mathbf{y}$ for $\mathbb{Z}_{p^2}^n$ with $-\frac{p^2-1}{2} \le y_i \le \frac{p^2-1}{2}$, $1 \le i \le n$. With this convention we can say

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

from which one readily obtains the well-known inequality

$$\sum_{\mathbf{y}} \left|a_{\mathcal{B}}(\mathbf{y})\right| \ll \log^n p.$$

Also, by Lemma 1 one has uniformly $|\phi(V_{p^2}, \mathbf{y})| \le p^{\frac{3}{2}n-1} + p^n$. The asymptotic formula in (1.3) is now an immediate consequence of the basic identity (2.1), and the fact that $a_{\mathcal{B}}(\mathbf{0}) = |\mathcal{B}|/p^{2n}$.

4 Proof of Theorem 1

We turn now to the proof of Theorem 1. Let $\mathcal{B}$ be a box of point of the type (1.2), with $0 < m_i \le p^2$, $1 \le i \le n$, and let $\chi_{\mathcal{B}}$ be its characteristic function with Fourier expansion

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

As usual, we define the convolution of two functions α, β defined on $\mathbb{Z}_{p^2}$ by

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

Lemma 3 *Let $\alpha = \chi_{\mathcal{B}} * \chi_{\mathcal{B}'}$, where $\mathcal{B}$ is a box as in* (1.2), *$\mathcal{B}' = \mathcal{B} - \mathbf{c}$, with $\mathbf{c}$ chosen so that $\mathcal{B}'$ is 'nearly' centered at the origin,*

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

Then, for any subset S of $\mathbb{Z}_{p^2}^n$, we have

$$\sum_{\mathbf{x} \in S} \alpha(\mathbf{x}) \ge \frac{1}{2^n} |\mathcal{B}| |S \cap \mathcal{B}|.$$

Proof Let

$$I = \{a_i, a_i + 1, \dots, a_i + m_i - 1\}.$$

Then if m_i is odd, $c_i = a_i + \frac{m_i-1}{2}$, and hence

$$I' = I - c_i = \left\{-\frac{m_i-1}{2}, \dots, \frac{m_i-1}{2}\right\}.$$

Thus, for any $x \in I$,

$$\sum_{\substack{u\in I \\ u+v=x}} \sum_{v\in I'} 1 \geq \frac{m_i+1}{2} \geq \frac{m_i}{2}.$$

If m_i is even, so that $c_i = a_i + \frac{m_i}{2} - 1$, then

$$I' = I - c_i = \left\{-\frac{m_i}{2} + 1, \dots, \frac{m_i}{2}\right\},$$

and so for any $x \in I$,

$$\sum_{\substack{u\in I \\ u+v=x}} \sum_{v\in I'} 1 \geq \frac{m_i}{2}.$$

Thus, for any $\mathbf{x} \in \mathcal{B}$, we have

$$\alpha(\mathbf{x}) \geq \prod_{i=1}^{n} \frac{m_i}{2} = 2^{-n}|\mathcal{B}|,$$

and so for any subset S of $\mathbb{Z}_{p^2}^n$,

$$\sum_{\mathbf{x}\in S} \alpha(\mathbf{x}) \geq \sum_{\mathbf{x}\in S\cap\mathcal{B}} \alpha(\mathbf{x}) \geq |S \cap \mathcal{B}| 2^{-n} |\mathcal{B}|.$$

□

With α as given in Lemma 3, we have by the fundamental identity, Lemma 2, that

$$\sum_{\mathbf{x}\in V_{p^2}} \alpha(\mathbf{x}) = p^{-2} \sum_{\mathbf{x}} \alpha(\mathbf{x}) + \underbrace{p^n \sum_{\substack{y_i=1 \\ p^2|Q^*(\mathbf{y})}}^{p^2} a(\mathbf{y})}_{E_0} - \underbrace{p^{n-1} \sum_{\substack{y_i=1 \\ p|Q^*(\mathbf{y})}}^{p^2} a(\mathbf{y})}_{E_1}$$
$$- \underbrace{\Delta p^{(3n/2)-2} \sum_{y_i'=1}^{p} a(p\mathbf{y}')}_{E_2} + \underbrace{\Delta p^{(3n/2)-1} \sum_{\substack{y_i'=1 \\ p|Q^*(\mathbf{y}')}}^{p^2} a(p\mathbf{y}')}_{E_3}.$$

Also,

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

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

and

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

It follows that

$$\sum_{\mathbf{x}\in V_{p^2}} \alpha(\mathbf{x}) \le \frac{|\mathcal{B}|^2}{p^2} + |E_0 - E_1| + |E_2 - E_3|. \tag{4.1}$$

By the Cauchy-Schwarz inequality and Parseval's identity (see, for example, [5, 6]), we get

$$\begin{aligned}
\sum_{\mathbf{y}} \bigl|a(\mathbf{y})\bigr| &= p^{2n} \sum_{\mathbf{y}} \bigl|a_{\mathcal{B}}(\mathbf{y}) a_{\mathcal{B}'}(\mathbf{y})\bigr| \\
&\le p^{2n} \Bigl(\sum_{\mathbf{y}} \bigl|a_{\mathcal{B}}(\mathbf{y})\bigr|^2 \Bigr)^{1/2} \Bigl(\sum_{\mathbf{y}'} \bigl|a_{\mathcal{B}'}(\mathbf{y}')\bigr|^2 \Bigr)^{1/2} \\
&\le p^{2n} \Bigl(\frac{1}{p^{2n}} \sum_{\mathbf{y}} \chi^2_{\mathcal{B}}(\mathbf{x}) \Bigr)^{1/2} \Bigl(\frac{1}{p^{2n}} \sum_{\mathbf{y}} \chi^2_{\mathcal{B}'}(\mathbf{x}) \Bigr)^{1/2} \\
&= |\mathcal{B}|^{1/2} \bigl|\mathcal{B}'\bigr|^{1/2} = |\mathcal{B}|.
\end{aligned} \tag{4.2}$$

Next

$$|E_0 - E_1| = \left| p^n \sum_{\substack{y_i=1 \\ p^2 | Q^*(\mathbf{y})}}^{p^2} a(\mathbf{y}) - p^{n-1} \sum_{\substack{y_i=1 \\ p | Q^*(\mathbf{y})}}^{p^2} a(\mathbf{y}) \right| = \left| \sum_{y_i=1}^{p^2} \psi(\mathbf{y}) a(\mathbf{y}) \right|, \tag{4.3}$$

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 (4.3) and using (4.2), we obtain

$$|E_0 - E_1| \le \bigl(p^n - p^{n-1}\bigr) \sum_{\mathbf{y}} \bigl|a(\mathbf{y})\bigr| \le \bigl(p^n - p^{n-1}\bigr) |\mathcal{B}|. \tag{4.4}$$

Also,

$$\begin{aligned}
|E_2 - E_3| &= \left| -\Delta p^{(3n/2)-2} \sum_{y'_i=1}^{p} a\bigl(p\mathbf{y}'\bigr) + \Delta p^{(3n/2)-1} \sum_{\substack{y'_i=1 \\ p | Q^*(\mathbf{y}')}}^{p} a\bigl(p\mathbf{y}'\bigr) \right| \\
&\le \left| \sum_{y'_i=1}^{p} \theta\bigl(\mathbf{y}'\bigr) a\bigl(p\mathbf{y}'\bigr) \right|,
\end{aligned} \tag{4.5}$$

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 (4.5),

$$|E_2 - E_3| \leq \left(p^{3n/2-1} - p^{3n/2-2}\right) \sum_{y_i'=1}^{p} \left|a\left(p\mathbf{y}'\right)\right|. \tag{4.6}$$

We are left with estimating $\sum_{|y_i|<p/2} |a_i(py_i)|$. Say $a(\mathbf{y}) = \prod_{i=1}^{n} a_i(y_i)$. Since the Fourier coefficients are given by $a(\mathbf{y}) = p^{2n} a_B(\mathbf{y}) a_{B'}(\mathbf{y})$, we have

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

and so

$$\left|a_i(py_i)\right| \leq \min\left\{\frac{m_i^2}{p^2}, \frac{1}{4y_i^2}\right\} \quad \text{for } |y_i| < p/2. \tag{4.7}$$

Lemma 4

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

Proof We begin by establishing the inequality

$$\sum_{|y_i|>p/2m_i} \frac{1}{4y_i^2} \leq \begin{cases} 4\frac{m_i}{p} & \text{if } m_i \leq p/2, \\ 1 & \text{if } m_i > p/2. \end{cases} \tag{4.8}$$

We split the proof of the inequality into two cases.

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

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

Thus,

$$\begin{aligned} \sum_{y=L}^{\infty} \frac{1}{4y^2} &= \frac{1}{4}\sum_{y=L}^{\infty} \frac{1}{y^2} \leq \frac{1}{4L^2} + \frac{1}{4}\int_L^{\infty} \frac{dx}{x^2} \\ &= \frac{1}{4L^2} + \frac{1}{4L} = \frac{1}{4L}\left(1 + \frac{1}{L}\right) \\ &\leq \frac{2}{4L} = \frac{1}{2L} \leq \frac{4m_i}{2p} = 2\frac{m_i}{p}, \end{aligned}$$

and 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

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

Returning to the proof of the lemma, we consider four cases as follows.

Case (i): If $m_i \le \frac{p}{2}$, then by (4.7) and (4.8) we have

$$\begin{aligned}\sum_{|y_i|<p/2} \left|a_i(py_i)\right| &\le \sum_{|y_i|\le p/2m_i} \frac{m_i^2}{p^2} + \sum_{|y_i|>p/2m_i} \frac{1}{4y_i^2} \\ &\le \frac{m_i^2}{p^2}\left(\frac{p}{m_i}+1\right) + \frac{4m_i}{p} = \frac{5m_i}{p} + \frac{m_i^2}{p^2} \le 6\frac{m_i}{p}.\end{aligned}$$

Case (ii): If $m_i > \frac{p}{2}$, then by (4.7) and (4.8)

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

Case (iii): If $\frac{p}{2} < m_i < p$, then continuing from Case (ii) we have

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

Case (iv): If $m_i > p$, then continuing from Case (ii) we get

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

completing the proof of Lemma 4. □

We return to the proof of Theorem 1. Suppose that

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

By Lemma 4, we obtain

$$\begin{aligned}\sum_{|\mathbf{y}|<p/2} \left|a_i(p\mathbf{y})\right| &= \prod_{i=1}^{n} \sum_{|y_i|<p/2} \left|a_i(py_i)\right| = \prod_{m_i\le p} 6\frac{m_i}{p} \prod_{m_i>p} 3\frac{m_i^2}{p^2} \\ &\le 3^n 2^l \frac{|\mathcal{B}|}{p^n} \prod_{m_i>p} \frac{m_i}{p} = 3^n 2^l \frac{|\mathcal{B}|}{p^n} \frac{\prod_{m_i>p} m_i}{p^{n-l}}.\end{aligned} \tag{4.9}$$

Using (4.9), then continuing from (4.6), we have

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

By (4.1) and (4.4), we then obtain

$$\begin{aligned} \sum_{\mathbf{x} \in V_{p^2}} \alpha(\mathbf{x}) &\le \frac{|\mathcal{B}|^2}{p^2} + |E_0 - E_1| + |E_2 - E_3| \\ &\le \frac{|\mathcal{B}|^2}{p^2} + \left(p^n - p^{n-1}\right)|\mathcal{B}| + 3^n 2^l p^{l-\frac{n}{2}-1} |\mathcal{B}| \prod_{i=1}^{n} m_i \\ &\le \frac{|\mathcal{B}|^2}{p^2} + p^n |\mathcal{B}| + 3^n 2^l p^{l-(n/2)-1} |\mathcal{B}| \prod_{i=l+1}^{n} m_i. \end{aligned} \tag{4.10}$$

The task now is to determine which of the terms $|\mathcal{B}|^2/p^2$, $p^n|\mathcal{B}|$ and $3^n 2^l p^{l-(n/2)-1}|\mathcal{B}| \times \prod_{i=l+1}^{n} m_i$ in (4.10) is the dominant term. We consider two cases as follows.

Case (i): Suppose $l \le \frac{n}{2} - 1$. Then, comparing the first and third terms, we get

$$\begin{aligned} \frac{3^n 2^l p^{l-(n/2)-1} |\mathcal{B}| \prod_{i=l+1}^{n} m_i}{|\mathcal{B}|^2/p^2} &= \frac{1}{|\mathcal{B}|} p^{l-(n/2)+1} 3^n 2^l \prod_{i=l+1}^{n} m_i \\ &\le \frac{p^{l-(n/2)+1} 3^n 2^l}{\prod_{i=1}^{l} m_i} \le 3^n 2^l p^{l-(n/2)+1} \le 3^n 2^l. \end{aligned}$$

This leads to

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

Case (ii): Suppose $l \ge \frac{n}{2}$. Then, comparing the second and third terms, we have

$$\begin{aligned} \frac{3^n 2^l p^{l-(n/2)-1} |\mathcal{B}| \prod_{i=l+1}^{n} m_i}{p^n |\mathcal{B}|} &= 3^n 2^l p^{l-(3n/2)-1} \prod_{i=l+1}^{n} m_i \\ &\le 3^n 2^l p^{l-(3n/2)-1} p^{2(n-l)} = 3^n 2^l p^{(n/2)-1-l} \le \frac{3^n 2^l}{p}. \end{aligned}$$

This gives that

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

So for any l, we always have

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

Returning to (4.10), we now can write

$$\begin{aligned}\sum_{\mathbf{x}\in V_{p^2}} \alpha(\mathbf{x}) &\leq \frac{|\mathcal{B}|^2}{p^2} + p^n|\mathcal{B}| + 3^n 2^l p^{l-(n/2)-1}|\mathcal{B}| \prod_{i=l+1}^{n} m_i \\ &\leq \frac{|\mathcal{B}|^2}{p^2} + p^n|\mathcal{B}| + 3^n 2^l \frac{|\mathcal{B}|^2}{p^2} + \frac{3^n 2^l}{p} p^n|\mathcal{B}| \\ &= \left(1 + 3^n 2^l\right)\frac{|\mathcal{B}|^2}{p^2} + \left(1 + \frac{3^n 2^l}{p}\right)p^n|\mathcal{B}| \\ &\leq \gamma_n'\left(\frac{|\mathcal{B}|^2}{p^2} + p^n|\mathcal{B}|\right), \end{aligned} \tag{4.11}$$

where $\gamma_n' = 1 + 3^n 2^l$. On the other hand, using Lemma 3, we have

$$\sum_{\mathbf{x}\in V_{p^2}} \alpha(\mathbf{x}) \geq \frac{1}{2^n}|\mathcal{B}||V_{p^2} \cap \mathcal{B}|. \tag{4.12}$$

Combining the last two inequalities ((4.11) and (4.12)) yields

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

where $\gamma_n = 1 + 6^n$. Theorem 1 is proved.

5 Proof of Theorem 2

Let $\mathcal{B}$ be a box of points in $\mathbb{Z}^n$ as given in (1.2). Partition $\mathcal{B}$ into $N = N_{\mathcal{B}}$ smaller boxes B_i,

$$\mathcal{B} = \mathrm{B}_1 \cup \mathrm{B}_2 \cup \cdots \cup \mathrm{B}_N,$$

where each B_i has all of its edge lengths $\leq p^2$. Plainly,

$$N_{\mathcal{B}} = \prod_{i=1}^{n}\left\lceil \frac{m_i}{p^2} \right\rceil.$$

Applying Theorem 1 to each B_i, we get

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

The proof of Theorem 2 is complete.

Competing interests
The author declares that they have no competing interests.

Acknowledgements
The author would like to thank his professor Todd Cochrane for suggesting the idea behind the statement of Lemma 3, which inspired the results of this paper. He would also like to thank the referees for their detailed comments and suggestions which improved the presentation of the results of this paper. Finally, the author would like to thank the VTEX Typesetting Services for their assistance in formatting and typesetting this paper.

Received: 19 September 2014 Accepted: 18 March 2015 Published online: 26 March 2015

References

1. Ayyad, A, Cochrane, T, Zheng, Z: The congruence $x_1x_2 \equiv x_3x_4 \pmod p$, the equation $x_1x_2 = x_3x_4$, and mean values of character sums. J. Number Theory **59**(2), 398-413 (1996)
2. Hakami, A: Small zeros of quadratic congruences to a prime power modulus. PhD thesis, Kansas State University (2009)
3. Hakami, A: Estimates for lattice points of quadratic forms with integral coefficients modulo a prime number square. J. Inequal. Appl. **2014**, 290 (2014). doi:10.1186/1029-242X-2014-290
4. Hakami, A, Cochrane, T: Small zeros of quadratic forms mod p^2. Proc. Am. Math. Soc. **140**(12), 4041-4052 (2012)
5. Cochrane, T: Small solutions of congruences. PhD thesis, University of Michigan (1984)
6. King, HL: Introduction to Number Theory. Springer, Berlin (1982)