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

Ali H Hakami*

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

Abstract
Let $Q(\mathbf{x}) = Q(x_1, x_2, \dots, x_n)$ be a nonsingular quadratic form with integer coefficients, n be even. Let $V = V_Q = V_{p^2}$ denote the set of zeros of $Q(\mathbf{x})$ in $\mathbb{Z}_{p^2}$, p be an odd prime, and $|V|$ denote the cardinality of V. In this paper, we are interested in giving an upper bound of the number of integer solutions of the congruence $Q(\mathbf{x}) \equiv 0 \pmod{p^2}$ in small boxes of the type $\{\mathbf{x} \in \mathbb{Z}^n_{p^2} | a_i \le x_i < a_i + m_i, 1 \le i \le n\}$ centered about the origin, where $a_i, m_i \in \mathbb{Z}$, and $0 < m_i < p^2$ for $1 \le i \le n$.
MSC: 11E04; 11E08; 11E12; 11P21

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

1 Introduction

Let $Q(\mathbf{x}) = Q(x_1, x_2, \dots, x_n) = \sum_{1 \le i \le j \le n} a_{ij} x_i x_j$ be a quadratic form with integer coefficients in n-variables, and $V = V_{p^2}(Q)$ 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 $(\cdot/p)$ 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

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

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 paper is stated in the following theorem.

Theorem 1 *Suppose n is even, Q is nonsingular* $\pmod p$, *and $V_{p^2,\mathbb{Z}} = V_{p^2,\mathbb{Z}}(Q)$ is the set of integer solutions of the congruence* (2). *Then for any box $\mathcal{B}$ of type* (1) *centered about the origin, if $\Delta_p = \pm 1$,*

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

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

$$\gamma_n = \begin{cases} 2^n(1 + \frac{2^{(n/2)+1}}{p}), & \Delta = -1, \\ 2^n(1 + 2^{(n/2)+1}), & \Delta = +1. \end{cases}$$

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

$$|V \cap \mathcal{B}| = \frac{|\mathcal{B}|}{p} + O\big(p^{n/2}(\log p)^{2n}\big), \tag{4}$$

for any box $\mathcal{B}$ (see [1]). It is apparent from (4) that $|V \cap \mathcal{B}|$ is nonempty provided

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

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. The key ingredient in obtaining the identity in (4) is a uniform upper bound on the function

$$\phi(V, \mathbf{y}) = \begin{cases} \sum_{\mathbf{x} \in V} e_{p^2}(\mathbf{x} \cdot \mathbf{y}) & \text{for } \mathbf{y} \neq \mathbf{0}, \\ |V| - p^{2(n-1)} & \text{for } \mathbf{y} = \mathbf{0}. \end{cases} \tag{5}$$

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

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

where

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

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

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

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

$$\sum_{\mathbf{x} \in V} \alpha(\mathbf{x}) = p^{-2n}|V| \sum_{\mathbf{x}} \alpha(\mathbf{x}) + \sum_{\mathbf{y} \neq \mathbf{0}} a(\mathbf{y}) \phi(V, \mathbf{y}), \tag{6}$$

where $\phi(V,\mathbf{y})$ is defined by (5). A variation of (6) that is sometimes more useful is

$$\sum_{\mathbf{x}\in V}\alpha(\mathbf{x}) = p^{-2}\sum_{\mathbf{x}}\alpha(\mathbf{x}) + \sum_{\mathbf{y}} a(\mathbf{y})\phi(V,\mathbf{y}), \tag{7}$$

which is obtained from (6) by noticing that $|V| = \phi(V,\mathbf{0}) + p^{2(n-1)}$, whence

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

Equations (6) and (7) 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 (6) or (7). One tries to make an optimal choice of $\alpha(\mathbf{x})$ in order to minimize the error term. Special cases of (6) and (7) have appeared a number of times in the literature for different types of algebraic sets V; see Chalk [2], Tietäväinen [3], and Myerson [4]. The first case treated was to let $\alpha(\mathbf{x})$ be the characteristic function $\chi_S(\mathbf{x})$ of a subset S of $\mathbb{Z}_{p^2}^n$, whence (7) gives rise to formulas of the type

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

Equation (4) is obtained in this manner. Particular attention has been given to the case where $S = \mathcal{B}$, a box of points in $\mathbb{Z}_{p^2}^n$. Another popular choice for α is to let it be a convolution of two characteristic functions, $\alpha = \chi_S * \chi_T$ for $S, T \subseteq \mathbb{Z}_{p^2}^n$. We recall that if $\alpha(\mathbf{x})$, $\beta(\mathbf{x})$ are complex valued functions defined on $\mathbb{Z}_{p^2}^n$, 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 $\mathbf{x}\in\mathbb{Z}_{p^2}^n$. If we take $\alpha(\mathbf{x}) = \chi_S * \chi_T(\mathbf{x})$ then it is clear from the definition that $\alpha(\mathbf{x})$ is the number of ways of expressing $\mathbf{x}$ as a sum $\mathbf{s}+\mathbf{t}$ with $\mathbf{s}\in S$ and $\mathbf{t}\in T$. Moreover, $(S+T)\cap V$ is nonempty if and only if $\sum_{\mathbf{x}\in V}\alpha(\mathbf{x}) > 0$.

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

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

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

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

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

$$\alpha * \beta(\mathbf{x}) = \sum_{\mathbf{y}} p^{2n} a(\mathbf{y}) b(\mathbf{y}) e_{p^2}(\mathbf{x}\cdot\mathbf{y}), \tag{8}$$

$$\alpha\beta(\mathbf{x}) = \alpha(\mathbf{x})\beta(\mathbf{x}) = \sum_{\mathbf{y}} (a * b)(\mathbf{y}) e_{p^2}(\mathbf{x}\cdot\mathbf{y}), \tag{9}$$

$$\sum_{\mathbf{x}} (\alpha * \beta)(\mathbf{x}) = \Bigl(\sum_{\mathbf{x}} \alpha(\mathbf{x})\Bigr)\Bigl(\sum_{\mathbf{x}} \beta(\mathbf{x})\Bigr), \tag{10}$$

$$\sum_{\mathbf{x}} \bigl|(\alpha * \beta)(\mathbf{x})\bigr| \le \Bigl(\sum_{\mathbf{x}} \bigl|\alpha(\mathbf{x})\bigr|\Bigr)\Bigl(\sum_{\mathbf{x}} \bigl|\beta(\mathbf{x})\bigr|\Bigr), \tag{11}$$

$$\sum_{\mathbf{y}} \bigl|a(\mathbf{y})\bigr|^2 = p^{-2n} \sum_{\mathbf{x}} \bigl|\alpha(\mathbf{x})\bigr|^2. \tag{12}$$

The last identity is Parseval's equality.

2 Fundamental identity

Let $Q(\mathbf{x}) = Q(x_1,\dots,x_n)$ 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 $S = \sum_{x=1}^{p^2} e_{p^2}(ax^2 + bx)$, one obtains the following.

Lemma 1 ([5, 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 $p|\mathbf{y}$. Then for any $\mathbf{y}$,*

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

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

Back to (7): we saw the identity

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

Inserting the value $\phi(V,\mathbf{y})$ in Lemma 1 yields (see [6]) the following.

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

$$\sum_{\mathbf{x}\in V}\alpha(\mathbf{x}) = p^{-2}\sum_{\mathbf{x}}\alpha(\mathbf{x}) + p^n\sum_{p^2|Q^*(\mathbf{y})}a(\mathbf{y}) - p^{n-1}\sum_{p|Q^*(\mathbf{y})}a(\mathbf{y}) - \Delta p^{(3n/2)-2}\sum_{\mathbf{y}' \pmod p}^{p}a(p\mathbf{y}') + \Delta p^{(3n/2)-1}\sum_{\substack{p|Q^*(\mathbf{y}')\\ \mathbf{y}' \pmod p}}a(p\mathbf{y}'). \tag{13}$$

3 Auxiliary lemma on estimating the sum $\sum_{y_i=1}^{p} a(p\mathbf{y})$

For later reference, we construct the following lemma on estimating the sum $\sum_{y_i}^{p} a(p\mathbf{y})$. Let $\mathcal{B}$ 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 $\mathbb{Z}_{p^2}^n$. Let $\chi_{\mathcal{B}}$ be its characteristic function with Fourier expansion $\chi_{\mathcal{B}}(\mathbf{x}) = \sum_{\mathbf{y}} a_{\mathcal{B}}(\mathbf{y})e_{p^2}(\mathbf{x}\cdot\mathbf{y})$. Let $\alpha(\mathbf{x}) = \chi_{\mathcal{B}} * \chi_{\mathcal{B}} = \sum_{\mathbf{y}} a(\mathbf{y})e_{p^2}(\mathbf{x}\cdot\mathbf{y})$. Then for any $\mathbf{y}\in\mathbb{Z}_{p^2}^n$,

$$a(\mathbf{y}) = p^{-2n}\prod_{i=1}^{n}\frac{\sin^2\pi m_i y_i/p^2}{\sin^2\pi y_i/p^2}, \tag{14}$$

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

$$m_1 \le m_2 \le \cdots \le m_l < p \le m_{l+1} \le \cdots \le m_n. \tag{15}$$

Then we have

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

Proof We first observe

$$\begin{aligned}\sum_{y_i=1}^{p} a(p\mathbf{y}) &= \sum_{y_i=1}^{p}\sum_{x_i=1}^{p^2}\frac{1}{p^{2n}}\alpha(\mathbf{x})e_{p^2}(-\mathbf{x}\cdot p\mathbf{y})\\ &= \sum_{x_i=1}^{p^2}\frac{1}{p^{2n}}\alpha(\mathbf{x})\sum_{y_i=1}^{p}e_p(-\mathbf{x}\cdot\mathbf{y})\\ &= \sum_{\substack{x_i=1\\ \mathbf{x}\equiv\mathbf{0} \pmod p}}^{p^2}\frac{p^n}{p^{2n}}\alpha(\mathbf{x})\\ &= \frac{1}{p^n}\sum_{\mathbf{x}\equiv\mathbf{0} \pmod p}\alpha(\mathbf{x})\end{aligned}$$

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

$$\le \frac{1}{p^n} \prod_{i=1}^{n} m_i \left(\left[\frac{m_i}{p} \right] + 1 \right). \tag{16}$$

To obtain the last inequality in (16) we must count the number of solutions of the congruence

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

with $\mathbf{u}, \mathbf{v} \in \mathcal{B}$. 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 (15) then, continuing from (16), we have

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

The lemma is established. □

4 Proof of Theorem 1

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

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

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

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

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

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

where

$$\gamma_n' = 1 + \frac{2^{(n/2)+1}}{p}.$$

Proof We begin by writing (13); we have the fundamental identity (mod p^2):

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

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

$$\sum_{\mathbf{y}} |a(\mathbf{y})| = p^{2n} \sum_{\mathbf{y}} |a_{\mathcal{B}}(\mathbf{y})|^2 = \sum_{\mathbf{y}} |\chi_{\mathcal{B}}(\mathbf{y})|^2 = |\mathcal{B}|. \tag{17}$$

Thus, it follows from (17) that

$$p^n \sum_{\substack{y_i=1 \\ p^2|Q^*(\mathbf{y})}}^{p^2} a(\mathbf{y}) \le p^n \sum_{\mathbf{y}} |a(\mathbf{y})| \le p^n |\mathcal{B}|. \tag{18}$$

Notice that the main term in (13) is

$$p^{-2}\sum_{\mathbf{x}} \alpha(\mathbf{x}) = p^{-2} \sum_{\mathbf{x}} \chi_{\mathcal{B}} * \chi_{\mathcal{B}}(\mathbf{x}) = \frac{|\mathcal{B}|^2}{p^2}. \tag{19}$$

By Lemma 3, we have

$$p^{(3n/2)-2} \sum_{y_i'=1}^{p} a(p\mathbf{y}') \le 2^{n-l} p^{l-(n/2)-2} |\mathcal{B}| \prod_{i=l+1}^{n} m_i \tag{20}$$

and

$$p^{(3n/2)-1} \sum_{\substack{y_i'=1 \\ p|Q^*(\mathbf{y}')}}^{p} a(p\mathbf{y}') \le p^{(3n/2)-1} \sum_{\mathbf{y}'} a(p\mathbf{y}') \le 2^{n-l} p^{l-(n/2)-1} |\mathcal{B}| \prod_{i=l+1}^{n} m_i, \tag{21}$$

where l, as defined before, is such that

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

Now going back to (13), if $\Delta = -1$, we have

$$\sum_{\mathbf{x}\in V_{p^2}} \alpha(\mathbf{x}) \le p^{-2}\sum_{\mathbf{x}} \alpha(\mathbf{x}) + p^n \sum_{\substack{y_i=1 \\ p^2|Q^*(\mathbf{y})}}^{p^2} a(\mathbf{y}) + p^{(3n/2)-2}\sum_{y_i'=1}^{p} a(p\mathbf{y}'). \tag{22}$$

Then, by the equality (19) and the inequalities in (18) and (20), we obtain

$$\sum_{\mathbf{x}\in V_{p^2}} \alpha(\mathbf{x}) \le \frac{|\mathcal{B}|^2}{p^2} + p^n|\mathcal{B}| + 2^{n-l}p^{l-(n/2)-2}|\mathcal{B}|\prod_{i=l+1}^{n} m_i. \tag{23}$$

We next determine which of the terms $|\mathcal{B}|^2/p^2$, $p^n|\mathcal{B}|$, and $2^{n-l}p^{l-(n/2)-2}|\mathcal{B}|\prod_{i=l+1}^{n} m_i$ in (23) is the dominant term. We consider two cases:

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

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

which implies that

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

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

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

which leads to

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

So for any l, always we have

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

Returning to (23), we now can write

$$\begin{aligned}\sum_{\mathbf{x}\in V_{p^2}} \alpha(\mathbf{x}) &\le \frac{|\mathcal{B}|^2}{p^2} + p^n|\mathcal{B}| + 2^{n-l}p^{l-(n/2)-2}|\mathcal{B}|\prod_{i=l+1}^{n} m_i \\ &\le \frac{|\mathcal{B}|^2}{p^2} + p^n|\mathcal{B}| + \frac{2^{(n/2)+1}}{p}\frac{|\mathcal{B}|^2}{p^2} + \frac{2^{n/2}}{p^2}p^n|\mathcal{B}| \\ &= \left(1+\frac{2^{(n/2)+1}}{p}\right)\frac{|\mathcal{B}|^2}{p^2} + \left(1+\frac{2^{n/2}}{p^2}\right)p^n|\mathcal{B}| \\ &\le \gamma_n'\left(\frac{|\mathcal{B}|^2}{p^2} + p^n|\mathcal{B}|\right), \end{aligned} \tag{24}$$

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

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

Hence it follows by combining (24) and (25) we find that

$$|\mathcal{B}\cap V_{p^2}| \le 2^n\gamma_n'\left(\frac{|\mathcal{B}|}{p^2} + p^n\right). \qquad \square$$

Lemma 5 *Let p be an odd prime, $V_{p^2} = V_{p^2}(Q)$ be the set of zeros of* (2) *in $\mathbb{Z}_{p^2}^n$, and $\mathcal{B}$ be a box as given in* (1) *centered at the origin with all $m_i \le p^2$. If $\Delta_p = +1$, then*

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

where

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

Proof If $\Delta_p = +1$, again by (13), we have

$$\begin{aligned}\sum_{\mathbf{x}\in V_{p^2}} \alpha(\mathbf{x}) &\le p^{-2}\sum_{\mathbf{x}}\alpha(\mathbf{x}) + p^n\sum_{\mathbf{y}}\left|a(\mathbf{y})\right| + p^{(3n/2)-1}\sum_{\mathbf{y}\ (\mathrm{mod}\ p)} a(p\mathbf{y}) \\ &\le \frac{|\mathcal{B}|^2}{p^2} + p^n|\mathcal{B}| + 2^{n-l}p^{l-(n/2)-1}|\mathcal{B}|\prod_{i=l+1}^{n} m_i. \end{aligned} \tag{26}$$

We do a similar investigation (as before) to determine which of the terms $|\mathcal{B}|^2/p^2$, $p^n|\mathcal{B}|$, and $2^{n-l}p^{l-(n/2)-1}|\mathcal{B}|\prod_{i=l+1}^{n} m_i$ of the inequality (26) is the dominant term. In case (i) we find

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

which means that

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

And in case (ii) we find

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

which gives us that

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

Hence for any l, we always have

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

Now on looking at (26), one easily deduces

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

where $\gamma_n'' = 1 + 2^{(n/2)+1}$. Thus by (27),

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

This leads to the proof of the lemma. □

Proof of Theorem 1 This theorem follows immediately from Lemma 4 and Lemma 5 by letting $\gamma_n = 2^n\gamma_n'$ if $\Delta = -1$ and $\gamma_n = 2^n\gamma_n''$ if $\Delta = +1$. Thus we see from (24) and (27) that for $\Delta = \pm 1$, one always has

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

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

Acknowledgements
The author would like to thank the anonymous referee for his helpful and constructive comments and suggestions. He would also like to thank the Editors for their generous comments and support during the review process. Finally, he would like to thank the VTEX Typesetting Services for their assistance in formatting and typesetting this paper.

Received: 30 June 2014 Accepted: 18 July 2014 Published: 18 Aug 2014

References
1. Cochrane, T: Small solutions of congruences. PhD thesis, University of Michigan (1984)
2. Chalk, JHH: The number of solutions of congruences in incomplete residue systems. Can. J. Math. **15**, 291-296 (1963)
3. Tietäväinen, A: On the Solvability of Equations in Incomplete Finite Fields. Ann. Unviv. Turku. Ser. AI, vol. 102, pp. 1-13 (1967)
4. Myerson, G: The distribution of rational points on varieties defined over a finite field. Mathematika **28**, 153-159 (1981)
5. Hakami, A: Small zeros of quadratic congruences to a prime power modulus. PhD thesis, Kansas State University (2009)
6. Hakami, A: Small zeros of quadratic forms mod p^2. Proc. Am. Math. Soc. **140**(12), 4041-4052 (2012)

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