Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
Vol. 22, 2016, No. 3, 54–67

Small primitive zeros of quadratic forms mod P^3

Ali H. Hakami

Department of Mathematics, Jazan University
P.O.Box 277, Postal Code: 45142, Saudi Arabia
e-mail: aalhakami@jazanu.edu.sa

Received: 18 December 2015 **Revised:** 27 May 2016 **Accepted:** 2 June 2016

Abstract: Let $Q(\mathbf{x}) = Q(x_1, x_2, ..., x_n)$ be a quadratic form with integer coefficients, p be an odd prime and $\|x\| = \max_i |x_i|$. A solution of the congruence $Q(\mathbf{x}) \equiv \mathbf{0} \pmod{p^3}$ is said to be a primitive solution if $p \nmid x_i$ for some i. We prove that if $p > A$, where $A = 5 \cdot 2^{41}$, then this congruence has a primitive solution, with $\|x\| < 34p^{3/2}$, provided that $n \geq 6$ is even and Q is nonsinqular $(\mathrm{mod} p)$. Moreover, similar result is proven for cube boxes centered at the origin with edges of arbitrary lengths. These two results are extension of the quadratic forms problems.
Keywords: Quadratic forms, Congruences, Small solutions.
AMS Classification: Primary 11D79, 11E08, 11H50, 11H55.

1 Introduction

Let $Q(\mathbf{x}) = Q(x_1, x_2, ..., x_n)$ 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 $\Delta_p(Q) = \left((-1)^{n/2} \det A_Q/p\right)$ 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 $(\mathrm{mod}\ p)$ if $p \nmid \det A_Q$.

Consider the congruence

$$Q(\mathbf{x}) \equiv 0 \pmod{m}, \tag{1.1}$$

where m is a positive integer. The problem of finding a small solution of (1.1) 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. Our interest in this paper is in finding a small primitive solution of (1.1) in the case where $m = p^3$, a solution $\mathbf{x}$ with $\gcd(x_1, ..., x_n, m) = 1$. A primitive solution is sought to rule out solutions of the type $p\mathbf{y}$ where $\mathbf{y}$ satisfies $Q(\mathbf{y}) \equiv 0 \pmod{p}$. For the quadratic form $Q(x) = x_1^2 + \cdots + x_n^2$, it is clear that any nonzero solution $\mathbf{x}$ of (1.1) 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, Schlickewi and Schmidt [17] proved that (1.1) 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 (1.1) 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 $m = p^3$ they use a solution of the type $p\mathbf{y}$ with $Q(\mathbf{y}) \equiv 0 \pmod{p}$.

Dealing with $m = p$, p an odd prime, Heath-Brown [15] obtained a nonzero solution of (1.1) 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, 20] generalized Heath-Brown's work to all finite fields. Cochrane, in a sequence of papers [1, 2, 3] improved this to $\|\mathbf{x}\| < \max\{2^{19}p^{1/2}, 2^{22}10^6\}$. The best constant available is due to Hakami [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 Hakami [8, Theorem 1] generalized Cochrane's method to find a primitive solution of (1.1) 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 geometric method) [6, 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].

Our interest in this paper is the case $m = p^3$ with p a prime, more specifically obtaining small primitive solutions of the congruence

$$Q(\mathbf{x}) \equiv 0 \pmod{p^3}. \tag{1.2}$$

To do that we shall generalize $(\bmod\ p)$ methods for obtaining a small primitive solution. Our main result is the following theorem.

Theorem 1. *For any odd prime p and nonsingular quadratic form $Q(\mathbf{x}) \pmod{p}$ with $n \geq 6$, n even, if $p > A$, where $A = 5 \cdot 2^{41}$, then there exists a primitive solution of (1.2) with*

$$\|\mathbf{x}\| \leq 2^5 p^{3/2} \tag{1.3}$$

Note that this bound is best possible (order $O\left((p^3)^{1/2}\right)$. A generalization of Theorem 1 to boxes centered at the origin is given in Corollary 1. Theorem 1 is an immediate consequence of Corollary 2

Remarks

1. In order to prove Theorem 1 we shall use method of exponential sums because this method has the advantage that it allows us to give estimates on the number of small primitive solutions.

2. The estimate occurring in (1.3) is the best possible obtained by the method given here, provided $\Delta_p(Q) = +1$ ($\Delta_p(Q)$ is defined above) and p is sufficiently large. Weaker bounds are obtained by the author in [9, Theorem 1] for the case $\Delta_p(Q) = -1$, $\|\mathbf{x}\| \ll p^{(3/2)+(3/n)}$. Note that in the case of $\Delta_p(Q) = -1$, the estimate $\|\mathbf{x}\| \ll p^{(3/2)+(3/n)}$ yields a primitive

solution of (1.3) with exponent tending to 3/2 for n tending to infinity. For a general prime power $m = p^k$ and nonsingular form $(\mathrm{mod} p^k)$ in $n \geq 4$ variables (n even) a primitive solution of size $\|\mathbf{x}\| \ll m^{(1/2)+(1/n)}$ is obtained [10, Theorem 1]

3. Our attempts to use the geometric method for congruences $(\mathrm{mod}\ p^3)$ or higher powers) have not been successful in obtaining primitive solutions of size $\sqrt{m}$.

4. For a general modulus the problem of obtaining a small primitive solution remains unexplored. The correct answer will depend on the rank of the quadratic form modulo each of the prime divisors of m. For instance, the smallest primitive solution of the congruence $p(x_1^2+x_2^2)+3p(x_3^2+x_4^2)+9(x_5^2-\lambda x_6^2) \equiv 0\ (\mathrm{mod}\, 9p)$, with $p > 3$ a prime and λ a quadratic nonresidue $(\mathrm{mod} p)$ has size $\|\mathbf{x}\| = p$.

2 Basic identities and lemmas

Henceforth, we shall assume that n is even, p is an odd prime, and that $Q(\mathbf{x})$ is a nonsingular quadratic form $(\mathrm{mod}\, p)$ with $\Delta_p(Q) = +1$. Let $e_{p^3}(\alpha) = e^{2\pi i\alpha/p^3}$. Let $V_{p^3} = V_{p^3}(Q)$ be the set of zeros of Q contained in $\mathbb{Z}_{p^3}^n$ and let $Q^*(\mathbf{y})$ be the quadratic form associated with inverse of the matrix for $Q\ (\mathrm{mod}\ p)$. For $\mathbf{y} \in \mathbb{Z}_{p^3}^n$ set

$$\phi(V_{p^3}, \mathbf{y}) = \begin{cases} \sum\limits_{\mathbf{x} \in V} e_{p^3}(\mathbf{x}\cdot\mathbf{y}) & \text{for} \quad \mathbf{y} \neq \mathbf{0}, \\ |V_{p^3}| - p^{3(n-1)} & \text{for} \quad \mathbf{y} \neq \mathbf{0}. \end{cases}$$

We abbreviate complete sums over $\mathbb{Z}_{p^3}^n$ and $\mathbb{Z}_p^n$ in the manner

$$\sum_{\mathbf{x}} = \sum_{\mathbf{x}\ \mathrm{mod}\ p^3} = \sum_{x_1=1}^{p^3} \cdots \sum_{x_n=1}^{p^3}, \qquad \sum_{\mathbf{x}\ \mathrm{mod}\ p} = \sum_{x_1=1}^{p} \cdots \sum_{x_n=1}^{p}.$$

The following lemma gives us a formula for $\phi(V_{p^3}, \mathbf{y})$.

Lemma 1. [11, Theorem 1] *Suppose n is even, Q is nonsingular* $(\mathrm{mod}\ p)$ *and $\Delta = \Delta_p(Q)$. For $\mathbf{y} \in \mathbb{Z}^n$, put $\mathbf{y}' = p^{-j}\mathbf{y}$ in case $p\,|\mathbf{y}$, (i.e., $p\,|y_i$ for all i). Then*

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

with

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

and

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

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

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 $\mathbb{Z}_{p^3}^n$ with Fourier expansion $\alpha(\mathbf{x}) = \sum_{\mathbf{y}} a(\mathbf{y}) e_{p^3}(\mathbf{x}\cdot\mathbf{y})$ where $a(\mathbf{y}) = p^{-3n}\sum_{\mathbf{x}} \alpha(\mathbf{x}) e_{p^3}(-\mathbf{x}\cdot\mathbf{y})$. Then

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

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

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

Also by noticing that $|V| = \phi(V_{p^3},\mathbf{0}) + p^{3(n-1)}$, we obtain that

$$\sum_{\mathbf{x}\in V}\alpha(\mathbf{x}) = p^{-3}\sum_{\mathbf{x}}\alpha(\mathbf{x}) + \sum_{\mathbf{y}} a(\mathbf{y})\phi(V,\mathbf{y}). \tag{2.1}$$

Inserting the value of $\phi(V_{p^3},\mathbf{y})$ from Lemma 1 in (2.1) we obtain (see [9, Lemma 2]

Lemma 2 (The fundamental identity)**.** *For any complex valued $\alpha(\mathbf{x})$ on $\mathbb{Z}_{p^3}^n$,*

$$\begin{aligned}\sum_{\mathbf{x}\in V_{p^3}}\alpha(\mathbf{x}) &= p^{-3}\sum_{\mathbf{x}}\alpha(\mathbf{x}) \\ &+ \underbrace{p^{3n/2}\sum_{\substack{y_i=1\\ p^3\mid Q^*(\mathbf{y})}}^{p^3} a(\mathbf{y})}_{Er_1} + \underbrace{p^{2n-1}\sum_{\substack{y_i=1\\ p^2\mid Q^*(\mathbf{y})}}^{p^2} a(p\mathbf{y})}_{Er_2} + \underbrace{p^{(5n/2)-2}\sum_{\substack{y_i=1\\ p\mid Q^*(\mathbf{y})}}^{p} a(p^2\mathbf{y})}_{Er_3} \\ &- \underbrace{p^{(3n/2)-1}\sum_{\substack{y_i=1\\ p^2\mid Q^*(\mathbf{y})}}^{p^3} a(\mathbf{y})}_{Er_4} - \underbrace{p^{2n-2}\sum_{\substack{y_i=1\\ p\mid Q^*(\mathbf{y})}}^{p^2} a(p\mathbf{y})}_{Er_5} - \underbrace{p^{(5n/2)-3}\sum_{y_i=1}^{p} a(p^2\mathbf{y})}_{Er_6}.\end{aligned} \tag{2.2}$$

3 Proof of Theorem 1

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

$$\mathcal{B} = \{\mathbf{x}\in\mathbb{Z}^n \mid a_i \leqslant x_i < a_i + m_i,\ \ 1\leqslant i\leqslant n\}, \tag{3.1}$$

where $a_i, m_i \in \mathbb{Z},\ 1 \leqslant m_i \leqslant p^2,\ 1 \leqslant i \leqslant n$. Thus the number of points in $\mathcal{B}$ is $|\mathcal{B}| = \prod_{i=1}^{n} m_i$. Consider the congruence

$$Q(\mathbf{x}) \equiv 0 \pmod{p^2}, \tag{3.2}$$

with $x \in \mathcal{B}$. Our first step is to obtain an upper bound on the number of solutions of (3.2) contained in any box. Let $V_{p^2,\mathbb{Z}} = V_{p^2,\mathbb{Z}}(Q)$ be the set of integer solutions of (3.2). First we treat the case where all $m_i \leqslant p^2$. By work of [12, Lemma 4], we obtain

Lemma 3. *Let p be an odd prime, $V_{p^2} = V_{p^2}(Q)$ be the set of zeros of (3.2) in $\mathbb{Z}_{p^2}^n$, and $\mathcal{B}$ be a box as given in (3.1) centered at the origin with all $m_i \leqslant p^2$, then*

$$|\mathcal{B} \cap V_{p^2}| \leqslant \gamma_n \left(\frac{|\mathcal{B}|}{p^2} + p^n \right), \tag{3.3}$$

where

$$\gamma = 2^n(1 + 2^{(n/2)+1}). \tag{3.4}$$

Next we consider larger boxes where the m_i may exceed p^2. We define

$$N_{\mathcal{B}} = \prod_{i=1}^{n} \left(\left[\frac{m_i}{p^2} \right] + 1 \right). \tag{3.5}$$

Partition the box $\mathcal{B}$ in (3.1) into $N = N_{\mathcal{B}}$ smaller boxes B_i,

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

where each B_i has all of its edge lengths $\leqslant p^2$. Thus Lemma 3 can be applied to each B_i. We obtain

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

Thus we have proved

Lemma 4. *Let $V_{p^2,\mathbb{Z}} = V_{p^2,\mathbb{Z}}(Q)$ be the set of integer solutions of the congruence (3.2). Then for any box $\mathcal{B}$ of type (3.1),*

$$|\mathcal{B} \cap V_{p^2,\mathbb{Z}}| \leqslant \gamma_n \left(\frac{|\mathcal{B}|}{p^2} + N_{\mathcal{B}} \ p^n \right), \tag{3.6}$$

where γ as defined in (3.4) and $N_{\mathcal{B}}$ in (3.5).

Let $\mathcal{B}$ be a box of points in $\mathbb{Z}^n$ as in (3.1) centered about the origin with all $m_i \leqslant p^3$, and view this box as a subset of $\mathbb{Z}_{p^3}^n$. Let $\chi_{\mathcal{B}}$ be its characteristic function with Fourier expansion $\chi_{\mathcal{B}}(\mathbf{x}) = \sum_{\mathbf{y}} a_{\mathcal{B}}(\mathbf{y}) e_{p^3}(\mathbf{x}\cdot\mathbf{y})$. Let $\alpha(\mathbf{x}) = \chi_{\mathcal{B}} * \chi_{\mathcal{B}} = \sum_{\mathbf{y}} a(\mathbf{y}) e_{p^3}(\mathbf{x}\cdot\mathbf{y})$. Then for any $\mathbf{y} \in \mathbb{Z}_{p^3}^n$,

$$a(\mathbf{y}) = p^{-3n} \prod_{i=1}^{n} \frac{\sin^2 \pi m_i y_i/p^3}{\sin^2 \pi y_i/p^3}, \tag{3.7}$$

where the term in the product is taken to be m_i^2 if $y_i = 0$. In particular, if we take $|y_i| \leqslant p^3/2$ for all i, then using the fact that $|\sin(x)| \geqslant \frac{2}{\pi}|x|$ for $|x| \leqslant \pi/2$, we have

$$a(\mathbf{y}) \leqslant p^{-3n} \prod_{i=1}^{n} \min\left\{ m_i^2, \left(\frac{p^3}{2y_i}\right)^2 \right\}. \tag{3.8}$$

Apply the fundamental identity (2.2) to $\alpha(\mathbf{x}) = \chi_{\mathcal{B}} * \chi_{\mathcal{B}}$ to get

$$\begin{aligned} \sum_{\mathbf{x}\in V_{p^3}} \alpha(\mathbf{x}) \geqslant & \underbrace{p^{-3} \sum_{\mathbf{x}} \alpha(\mathbf{x})}_{\text{Main Term}} \\ & \underbrace{- p^{(3n/2)-1} \sum_{\substack{y_i=1 \\ p^2 | Q^*(\mathbf{y})}}^{p^3} a(\mathbf{y})}_{Er_4} \underbrace{- p^{2n-2} \sum_{\substack{y_i=1 \\ p | Q^*(\mathbf{y})}}^{p^2} a(p\mathbf{y})}_{Er_5} \underbrace{- p^{(5n/2)-3} \sum_{y_i=1}^{p} a(p^2\mathbf{y})}_{Er_6}, \end{aligned} \tag{3.9}$$

since Fourier coefficients $a(\mathbf{y})$ are all positive. The main term in (3.9) is

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

and the others are error terms.

For later reference, we construct a series of lemmas.

Lemma 5. *Let $\mathcal{B}$ be any box of type (3.1) viewed as a subset of $\mathbb{Z}_{p^3}^n$ and $\alpha(\mathbf{x}) = \chi_{\mathcal{B}} * \chi_{\mathcal{B}}(\mathbf{x})$. Then we have*

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

Proof. First,

$$\begin{aligned} \sum_{y_i=1}^{p^2} a(p\mathbf{y}) &= \sum_{y_i=1}^{p^2} \sum_{x_i=\mathbf{1}}^{p^3} \frac{1}{p^{3n}} \alpha(\mathbf{x}) e_{p^3}(-\mathbf{x}\cdot p\mathbf{y}) \\ &= \sum_{x_i=1}^{p^3} \frac{1}{p^{3n}} \alpha(\mathbf{x}) \sum_{y_i=1}^{p^2} e_{p^2}(-\mathbf{x}\cdot\mathbf{y}) \end{aligned}$$

$$= \frac{1}{p^{3n}} \sum_{\substack{x_i=1 \\ \mathbf{x}\equiv 0 \ (\mathrm{mod}\ p^2)}}^{p^2} \alpha(\mathbf{x}) p^{2n}$$
$$= \frac{1}{p^n} \sum_{\mathbf{x}\equiv 0 \ (\mathrm{mod}\ p^2)} \alpha(\mathbf{x})$$
$$= \frac{1}{p^n} \sum_{\substack{\mathbf{u}\in\mathcal{B} \\ \mathbf{u}+\mathbf{v}\equiv 0 \ (\mathrm{mod}\ p^2)}} \sum_{\mathbf{v}\in\mathcal{B}} 1. \tag{3.10}$$

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

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

with $\mathbf{u}, \mathbf{v} \in \mathcal{B}$. In fact for each choice of $\mathbf{v}$, there are at most $\prod_{i=1}^n ([m_i/p^2] + 1)$ cho-ices for $\mathbf{u}$. So the total number of solutions is less than or equal to $\prod_{i=1}^n m_i([m_i/p^2] + 1)$. It follows from (3.10),

$$\sum_{y_i=1}^{p^2} a(p\mathbf{y}) \ \leqslant \frac{1}{p^n} \prod_{i=1}^n m_i \left(\left[\frac{m_i}{p^2} \right] + 1 \right). \tag{3.11}$$

We split the product in (3.11) to get

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

and so

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

proving the lemma. □

Lemma 6. *Let $\mathcal{B}$ be any box of type (3.1) and $\alpha(\mathbf{x}) = \chi_{\mathcal{B}} * \chi_{\mathcal{B}}(\mathbf{x})$. Then we have*

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

Proof. We proceed as in the proof of the preceding lemma. First we observe that

$$\sum_{y_i=1}^{p} a(p^2\mathbf{y}) = \sum_{y_i=1}^{p} \sum_{x_i=\mathbf{1}}^{p^3} \frac{1}{p^{3n}} \alpha(\mathbf{x}) e_{p^3}(-\mathbf{x}\cdot p^2\mathbf{y})$$
$$= \sum_{x_i=1}^{p^3} \frac{1}{p^{3n}} \alpha(\mathbf{x}) \sum_{y_i=1}^{p} e_p(-\mathbf{x}\cdot\mathbf{y})$$
$$= \sum_{\substack{x_i=1 \\ \mathbf{x}\equiv 0 \ (\mathrm{mod}\ p)}}^{p^3} \frac{p^n}{p^{3n}} \alpha(\mathbf{x})$$

$$= \frac{1}{p^{2n}} \sum_{\mathbf{x} \equiv 0 \ (\mathrm{mod}\ p)} \alpha(\mathbf{x})$$
$$= \frac{1}{p^{2n}} \sum_{\substack{\mathbf{u} \in \mathcal{B} \\ \mathbf{u}+\mathbf{v} \equiv 0 \ (\mathrm{mod}\ p)}} \sum_{\mathbf{v} \in \mathcal{B}} 1$$
$$\leqslant \frac{1}{p^{2n}} \prod_{i=1}^{n} m_i \left(\left[\frac{m_i}{p} \right] + 1 \right). \tag{3.12}$$

The last inequality in (3.12) is true by the same reason given in the proof of the Lemma 5. Now we split the product in (3.12) to get

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

and thus we deduce

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

finishing the proof. □

Now we can proceed to estimate the error terms Er_4, Er_5 and Er_6 in (3.9). First we consider

$$Er_4 = p^{(3n/2)-1} \sum_{\substack{y_i'=1 \\ Q^*(\mathbf{y}) \equiv 0 \ (\mathrm{mod}\ p^2)}}^{p^3} a(\mathbf{y}'). \tag{3.13}$$

Let $\sum^*$ be an abbreviation for $\sum_{\mathbf{y}(\ \mathrm{mod}\ p^3),\ Q^*(\mathbf{y}) \equiv 0 (\ \mathrm{mod}\ p^2)}$. Define ρ_i by

$$\rho_i = \begin{cases} 2^{k_i - 1} & \text{for} \quad k_i \geqslant 1, \\ 0 & \text{for} \quad k_i = 0. \end{cases} \tag{3.14}$$

Using (3.8) yields

$$\sum_{\substack{\mathbf{y} \ (\mathrm{mod}\ p^3) \\ Q^*(\mathbf{y}) \equiv 0 \ (\mathrm{mod}\ p^2)}} |a(\mathbf{y})| \leqslant \sum_{k_1=0}^{\infty} \cdots \sum_{k_n=0}^{n} \sum_{\rho_i p^3/m_i \leqslant |y_i| \leqslant 2^{k_i} p^3/m_i}^{*} \prod_{i=1}^{n} \min \left\{ \frac{m_i^2}{p^3}, \frac{p^3}{4y_i^2} \right\}$$
$$\leqslant \sum_{k_1=0}^{\infty} \cdots \sum_{k_n=0}^{\infty} \sum_{|y_i| \leqslant 2^{k_i} p^3/m_i}^{*} \prod_{i=1}^{n} \frac{p^3}{4(2^{k_i-1}p^3/m_i)^2}$$
$$= \frac{|\mathcal{B}|^2}{p^{3n}} \sum_{k_1=0}^{\infty} \cdots \sum_{k_n=0}^{\infty} \sum_{|y_i| \leqslant 2^{k_i} p^3/m_i}^{*} \prod_{i=1}^{n} \frac{1}{2^{2k_i}}. \tag{3.15}$$

For non-negative integers $k_1, k_2, ..., k_n$, let

$$\mathcal{B}' = \left\{ \mathbf{y} \in \mathbb{Z}_{p^3}^n \,\middle|\, |y_i| \leqslant 2^{k_i} \frac{p^3}{m_i},\ 1 \leqslant i \leqslant n \right\}.$$

Set

$$m_i' = 2\left[\frac{2^{k_i}p^3}{m_i}\right] + 1.$$

Then it follows that

$$|\mathcal{B}'| = \prod_{i=1}^{n} m_i' \leqslant \prod_{i=1}^{n}\left(\frac{2^{k_i+1}p^3}{m_i} + 1\right) \leqslant \prod_{i=1}^{n}\frac{2^{k_i+2}p^3}{m_i}. \tag{3.16}$$

By the inequality (3.6) in Lemma 4, we have the upper bound

$$|\mathcal{B}' \cap V_{p^2,\mathbb{Z}}| \leqslant \gamma_n\frac{|\mathcal{B}'|}{p^2} + \gamma_n N_{\mathcal{B}'}\, p^n, \tag{3.17}$$

where by (3.5),

$$N_{\mathcal{B}'} = \prod_{i=1}^{n}\left(\left[\frac{m_i'}{p^2}\right] + 1\right) = \prod_{\substack{i=1\\ 2^{k_i} \geqslant m_i/4p}}^{n}\left(\left[\frac{m_i'}{p^2}\right] + 1\right). \tag{3.18}$$

The equality in (3.18) is true by the following implication:

$$2^{k_i} < \frac{m_i}{4p} \quad \Rightarrow \quad \frac{2^{k_i+2}p^3}{m_i} < p^2 \quad \Rightarrow \quad m_i' < p^2.$$

But the right -hand side of (3.18), is less than or equal to

$$\prod_{\substack{i=1\\ 2^{k_i} \geqslant m_i/4p}}^{n}\left(\frac{2^{k_i+1}p}{m_i} + \frac{1}{p^2} + 1\right) \leqslant 2^n \prod_{\substack{i=1\\ 2^{k_i} \geqslant\, m_i/4p}}^{n}\left(\frac{2^{k_i}p}{m_i} + 1\right).$$

So that

$$N_{\mathcal{B}'} \leqslant 2^n \prod_{\substack{i=1\\ 2^{k_i} \geqslant m_i/4p}}^{n}\left(\frac{2^{k_i}p}{m_i} + 1\right). \tag{3.19}$$

Apply the upper bound (3.17) to the inner sum $\sum_{\mathbf{y}}^{*}$ in (3.15), to obtain

$$\begin{aligned}\sum_{\substack{Q^*(\mathbf{y}) \equiv 0(\bmod p^2)\\ |y_i| \leqslant p^2/2}} |a(\mathbf{y})| &= \frac{|\mathcal{B}|^2}{p^{3n}}\sum_{k_1=0}^{\infty}\cdots\sum_{k_n=0}^{\infty}|\mathcal{B}' \cap V_{p^2,\mathbb{Z}}|\prod_{i=1}^{n}\frac{1}{2^{2k_i}}\\ &\leqslant \frac{|\mathcal{B}|^2}{p^{3n}}\sum_{k_1=0}^{\infty}\cdots\sum_{k_n=0}^{\infty}\left(\gamma_n\frac{|\mathcal{B}'|}{p^2} + \gamma_n N_{\mathcal{B}'}\, p^n\right)\prod_{i=1}^{n}\frac{1}{2^{2k_i}}\\ &\leqslant S_1 + S_2, \end{aligned}\tag{3.20}$$

say. Then by the inequality (3.16),

$$S_1 = \frac{|\mathcal{B}|^2}{p^{3n}}\sum_{k_1=0}^{\infty}\cdots\sum_{k_n=0}^{\infty}\left(\prod_{i=1}^{n}\frac{1}{2^{2k_i}}\right)\gamma_n\frac{\prod_{i=1}^{n}\frac{2^{k_i+2}p^3}{m_i}}{p^2}$$

$$\leqslant \frac{|\mathcal{B}|^2}{p^{3n}}\frac{\gamma_n}{p^2}\sum_{k_1=0}^{\infty}\cdots\sum_{k_n=0}^{\infty}\left(\prod_{i=1}^{n}\frac{1}{2^{2k_i}}\frac{2^{k_i+2}p^3}{m_i}\right)$$
$$\leqslant 4^n\gamma_n\frac{|\mathcal{B}|^2}{p^{3n+2}}\frac{p^{3n}}{|\mathcal{B}|}\prod_{i=1}^{n}\left(\sum_{k_i}\frac{1}{2^{k_i}}\right)$$
$$= 2^{3n}\gamma_n\frac{|\mathcal{B}|}{p^2}, \tag{3.21}$$

and by the inequality (3.19),

$$S_2 = \frac{|\mathcal{B}|^2}{p^{3n}}\sum_{k_1=0}^{\infty}\cdots\sum_{k_n=0}^{\infty}\gamma_n N_{\mathcal{B}'}p^n\prod_{i=1}^{n}\frac{1}{2^{2k_i}}$$
$$= 2^n\gamma_n\frac{|\mathcal{B}|^2}{p^{3n}}p^n\sum_{k_1=0}^{\infty}\cdots\sum_{k_n=0}^{\infty}\prod_{\substack{i=1\\ 2^{k_i}\geqslant m_i/4p}}^{n}\left(\frac{2^{k_i}p}{m_i}+1\right)\prod_{i=1}^{n}\frac{1}{2^{2k_i}}$$
$$= 2^n\gamma_n\frac{|\mathcal{B}|^2}{p^{3n}}p^n\prod_{i=1}^{n}\left[\sum_{\substack{k_i=0\\ 2^{k_i}<m_i/4p}}^{\infty}\frac{1}{2^{2k_i}}+\sum_{\substack{k_i\\ 2^{k_i}\geqslant m_i/4p}}\left(\frac{2^{k_i}p}{m_i}+1\right)\frac{1}{2^{2k_i}}\right]$$
$$\leqslant 2^n\gamma_n\frac{|\mathcal{B}|^2}{p^{2n}}\prod_{i=1}^{n}\left[\sum_{k_i=0}^{\infty}\frac{1}{2^{2k_i}}+\sum_{\substack{k_i\\ 2^{k_i}\geqslant m_i/4p}}\frac{p}{2^{k_i}m_i}\right]$$
$$= 2^n\gamma_n\frac{|\mathcal{B}|^2}{p^{2n}}\prod_{i=1}^{n}\left[\frac{4}{3}+\frac{2p^2}{m_i}\right]$$
$$\leqslant 2^n\gamma_n\frac{|\mathcal{B}|^2}{p^{2n}}\prod_{i=1}^{n}\left(\frac{4}{3}+\frac{2p}{m_i}\right)$$
$$\leqslant 2^n\gamma_n\frac{|\mathcal{B}|^2}{p^{2n}}\left(\prod_{m_i\leqslant p}\frac{4p}{m_i}\right)\left(\prod_{m_i>p}\frac{10}{3}\right)$$
$$\leqslant 8^n\gamma_n\frac{|\mathcal{B}|^2}{p^{2n}}\prod_{m_i\leqslant p}\left(\frac{p}{m_i}\right). \tag{3.22}$$

Thus by inequalities (3.13), (3.20), (3.21) and (3.22), we have

$$Er_4 \leqslant p^{(3n/2)-1}\left[2^{3n}\gamma_n\frac{|\mathcal{B}|}{p^2}\right]+p^{(3n/2)-1}\left[8^n\gamma_n\frac{|\mathcal{B}|^2}{p^{2n}}\prod_{m_i\leqslant p}\frac{p}{m_i}\right]$$
$$= \underbrace{2^{3n}\gamma_n p^{(3n/2)-3}\,|\mathcal{B}|}_{Er_{4,1}}+\underbrace{8^n\gamma_n\frac{|\mathcal{B}|^2}{p^{(n/2)+1}}\prod_{m_i\leqslant p}\frac{p}{m_i}}_{Er_{4,2}}.$$

From Lemma 5 and Lemma 6, it is follows readily that

$$Er_5 \leqslant p^{2n-2}\sum_{y_i'=1}^{p^2}a(p\mathbf{y}') \leqslant p^{n-2}\,|\mathcal{B}|\prod_{m_i\geqslant p^2}\frac{2m_i}{p^2},$$

and

$$Er_6 \leqslant p^{(5n/2)-3} \sum_{y_i'=1}^{p} a(p^2\mathbf{y}') \leqslant p^{(n/2)-3} |\mathcal{B}| \prod_{m_i \geqslant p} \frac{2m_i}{p}.$$

Summarizing our findings, we obtain

Proposition 1. *Assume that $n \geqslant 4$ is even, $V_{p^3} = V_{p^3}(Q)$, $\mathcal{B} \subseteq \mathbb{Z}_{p^3}^n$ is a box centered at the origin and $\alpha(\mathbf{x}) = \chi_{\mathcal{B}} * \chi_{\mathcal{B}}(\mathbf{x})$. Then*

$$\sum_{\mathbf{x} \in V_{p^3}} \alpha(\mathbf{x}) \geqslant \frac{|\mathcal{B}|^2}{p^3} - |Error|,$$

where

$$|Error| < \underbrace{2^{3n}\gamma_n p^{(3n/2)-3} |\mathcal{B}|}_{Er_{4,1}} + \underbrace{\gamma_n 8^n \frac{|\mathcal{B}|^2}{p^{(n/2)+1}} \prod_{m_i \leqslant p} \frac{p}{m_i}}_{Er_{4,2}}$$
$$+ \underbrace{p^{n-2} |\mathcal{B}| \prod_{m_i \geqslant p^2} \frac{2m_i}{p^2}}_{Er_5} + \underbrace{p^{(n/2)-3} |\mathcal{B}| \prod_{m_i \geqslant p} \frac{2m_i}{p}}_{Er_6}.$$

In what follows we compare each error term in Proposition 1 to the main term $|\mathcal{B}|^2/p^3$. Of course, we are seeking to make the left-hand side positive, so we make each of these error term less than $1/5$ of the main term. For the error term $Er_{4,1}$, we need

$$\frac{1}{5}\frac{|\mathcal{B}|^2}{p^3} \geqslant 2^{3n}\gamma_n p^{(3n/2)-3} |\mathcal{B}| \iff |\mathcal{B}| \geqslant 5 \cdot 2^{3n}\gamma_n p^{3n/2}. \tag{3.23}$$

For the error term $Er_{4,2}$,

$$\frac{1}{5}\frac{|\mathcal{B}|^2}{p^3} \geqslant \gamma_n 8^n \frac{|\mathcal{B}|^2}{p^{(n/2)+1}} \prod_{m_i \leqslant p} \frac{p}{m_i} \iff p^{(n/2)-2} \geqslant 5\gamma_n 8^n \prod_{m_i < p} \frac{p^2}{m_i}. \tag{3.24}$$

For the error term Er_5, we require that

$$\frac{1}{5}\frac{|\mathcal{B}|^2}{p^3} \geqslant p^{n-2} |\mathcal{B}| \prod_{m_i \geqslant p^2}^{n} \frac{2m_i}{p^2} \iff |\mathcal{B}| \geqslant 5p^{n+1} \prod_{m_i \geqslant p^2} \frac{2m_i}{p^2}. \tag{3.25}$$

Finally, for the error term Er_6,

$$\frac{1}{5}\frac{|\mathcal{B}|^2}{p^3} \geqslant p^{(n/2)-3} |\mathcal{B}| \prod_{m_i \geqslant p} \frac{2m_i}{p} \iff |\mathcal{B}| \geqslant 5p^{n/2} \prod_{m_i \geqslant p} \frac{2m_i}{p}. \tag{3.26}$$

If the inequalities in (3.24), (3.25), (3.26) and (3.27) hold, then there exist solutions for the congruence (1.2)

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

in $\mathcal{B} + \mathcal{B}$. This is the content of the next theorem.

Theorem 2. *Suppose that $n \geqslant 6$ is even, $\mathcal{B} \subseteq \mathbb{Z}_{p^3}^n$ is a box centered at the origin and $\alpha(\mathbf{x}) = \chi_{\mathcal{B}} * \chi_{\mathcal{B}}(\mathbf{x})$. If (3.24), (3.25), (3.26) and (3.27) hold, then*

$$\sum_{\mathbf{x}\in V} \alpha(\mathbf{x}) > \frac{1}{5}\frac{|\mathcal{B}|^2}{p^3}.$$

In particular

$$|V \cap (\mathcal{B}+\mathcal{B})| > \frac{|\mathcal{B}|}{5p^3}.$$

The condition $n \geqslant 6$ is placed in Theorem 2 because when $n = 4$ condition (3.25) always fails. The second inequality in the theorem follows from the fact that $\alpha(\mathbf{x})$ is supported on $\mathcal{B}+\mathcal{B}$ and $\alpha(\mathbf{x}) \leqslant |\mathcal{B}|$ for all $\mathbf{x}$. The next corollary demonstrates the existence of a primitive solution of the congruence (1.2).

Corollary 1. *Under the hypotheses of Theorem 2, $\mathcal{B}+\mathcal{B}$ contains a primitive solution of (1.2).*

Proof. First, recall that a solution of (1.2) is called primitive if some coordinate is not divisible by p. We shall write $p\,|\mathbf{x}$ for imprimitive points. Thus to prove this corollary we must prove

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

As in the proof of Lemma 6, we can write

$$\sum_{\substack{\mathbf{x}\in V\\ p|\mathbf{x}}} \alpha(\mathbf{x}) \leqslant \sum_{\substack{p|x_i\,,\\ 1\leqslant i\leqslant n}} \alpha(\mathbf{x}) = \sum_{\substack{\mathbf{u}\in\mathcal{B}\ \mathbf{v}\in\mathcal{B}\\ \mathbf{u}+\mathbf{v}\equiv 0(\bmod p)}}\sum 1 \leqslant \prod_{i=1}^{n} m_i \left(\left[\frac{m_i}{p}\right]+1\right) \leqslant |\mathcal{B}| \prod_{m_i\geqslant p} \frac{2m_i}{p}. \tag{3.27}$$

We claim that the latter quantity is less than $|\mathcal{B}|^2/5p^3$ for $n \geqslant 6$. Indeed, by our hypothesis (3.27), we have

$$\prod_{m_i\geqslant p} \frac{2m_i}{p} \leqslant \frac{|\mathcal{B}|}{5p^{n/2}}.$$

Since $n \geqslant 6$, the latter quantity is $\leqslant |\mathcal{B}|/5p^3$. On the other hand Theorem 2 yields,

$$\sum_{\mathbf{x}\in V} \alpha(\mathbf{x}) > \frac{|\mathcal{B}|^2}{5p^3}.$$

We therefore obtain

$$\sum_{\substack{\mathbf{x}\in V\\ p|\mathbf{x}}} \alpha(\mathbf{x}) > \frac{|\mathcal{B}|^2}{5p^3} - \sum_{\substack{\mathbf{x}\in V\\ p|\mathbf{x}}} \alpha(\mathbf{x}) > 0,$$

completing our proof. □

In connection with Theorem 2 we study the following special case when the box $\mathcal{B}$ is a cube.

Corollary 2. *Suppose $n \geqslant 6$ and $p > 5^{2/(n-4)}2^{10n/(n-4)}\gamma_n^{2/(n-4)}$, (where γ_n is given in (3.4)). Let $\mathcal{B}$ be a cube centered at the origin with all $m_i = B$, $B > 2^3 5^{1/n}\gamma_n^{1/n}p^{3/2}$. Then $\mathcal{B}+\mathcal{B}$ contains a primitive solution of (1.2).*

Proof. We may assume $B = \lceil 2^3 5^{1/n} \gamma_n^{1/n} p^{3/2} \rceil$ ("$\lceil\rceil$" denoting the smallest integer greater than or equal to B). In particular, since $p > 5^{2/(n-4)} 2^{10n/(n-4)} \gamma_n^{2/(n-4)}$ we have $p^{3/2} < B < p^2$. We need to check that the hypotheses of Theorem 2 are satisfied. Indeed,

$$(3.24) \iff B^n > 5 \cdot 2^{3n} \gamma_n p^{3n/2} \iff B > 5^{1/n} 2^3 \gamma_n^{1/n} p^{3/2},$$

$$(3.25) \iff 5^{-1} (3.27)^{-n} \gamma_n^{-1} p^{(n/2)-2} \geqslant \prod_{m_i < p} \frac{p^2}{m_i} \prod_{p < m_i < p^{3/2}} \frac{p^3}{m_i^2} = 1 \cdot 1$$
$$\iff p > 5^{2/(n-4)} (3.27)^{2n/(n-4)} \gamma_n^{2/(n-4)},$$

$$(3.26) \iff B^n > 5p^{n+1} \prod_{m_i \geqslant p^2} \frac{2m_i}{p^2} \iff B^n > 5p^{n+1}, \text{ since } B < p^2$$
$$\iff B > 5^{1/n} p^{1+(1/n)},$$

and

$$(3.27) \iff B^n \geqslant 5p^{n/2} \prod_{m_i \geqslant p} \frac{2m_i}{p} = 5p^{n/2} \frac{2^n B^n}{p^n} \iff p > 4 \cdot 5^{2/n}.$$

Thus the hypotheses of Theorem 2 are satisfied, and so Corollary 1 applies.

Proof of Theorem 1. If $p < 5 \cdot 2^{41}$, the result is trivial. Next note that for $n \geqslant 6$,

$$5^{2/(n-4)} 2^{10n/(n-4)} \gamma_n^{2/(n-4)} \leqslant 5 \cdot 2^{30} \cdot 2^6 (1 + 2^4) < 5 \cdot 2^{41}.$$

Thus, if $p > 5 \cdot 2^{41}$, the first hypothesis of Corollary 2 holds. The second hypothesis holds provided that $B \geqslant 34 \cdot p^{3/2}$. In this case we get a primitive solution with $\|\mathbf{x}\| < 34 p^{3/2}$. □

Acknowledgements

This paper has benefited from several remarks and suggestions by Professor Todd Cochrane (KSU). The author is very grateful to him.

References

[1] Cochrane, T. (1989) Small zeros of quadratic forms modulo p, *J. Number Theory*, 33(3), 286–292.

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

[3] Cochrane, T. (1991) Small zeros of quadratic forms modulo p, III, *J. Number Theory*, 33(1), 92–99.

[4] Cochrane, T. (1990) Small zeros of quadratic congruences modulo pq, *Mathematika*, 37(2), 261–272.

[5] Cochrane, T. (1995) Small zeros of quadratic congruences modulo pq, II, *J. Number Theory*, 50(2), 299–308.

[6] Cochrane, T. & Hakami, A. (2012) Small zeros of quadratic congruences modulo p^2, II, *Proceedings of the American Mathematical Society*, 140(12), 4041–4052.

[7] Hakami, A. (2009) *Small zeros of quadratic congruences to a prime power modulus*, Ph.D. thesis, Kansas State University.

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

[9] Hakami, A. (2011) Small zeros of quadratic forms modulo p^3, *Advances and Applications in Mathematical Sciences*, 9(1), 47–69.

[10] Hakami, A. (2015) Small primitive zeros of quadratic forms modulo p^m, *The Ramanujan Journal*, 38, 189–198.

[11] Hakami, A. (2011) On Cochrane's estimate for small zeros of quadratic forms modulo p, *Far East J. Math. Sciences*, 50(2), 151–157.

[12] Hakami, A. (2011) Lattice points of quadratic forms with Integral coefficents modulo p^2, *Pacific-Asian Journal of Mathematics*, 5(2), 145–164.

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

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

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

[16] Heath-Brown, D. R. (1991) Small solutions of quadratic congruences II, *Mathematika*, 38(2), 264–284.

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

[18] Wang, Y. (1990) On small zeros of quadratic forms over finite fields, *Algebraic Structures and Number Theory* (Hong Kong, 1988), 269–274, World Sci. Publ., Teaneck, NJ.

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

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