Journal of Algebra, Number Theory: Advances and Applications
Volume 6, Number 1-2, 2011, Pages 1-17

AN UPPER BOUND FOR THE NUMBER OF INTEGRAL SOLUTIONS OF QUADRATIC FORMS MOD *P*

ALI H. HAKAMI

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

Abstract

Let $Q(\mathbf{x}) = Q(x_1, x_2, \ldots, x_n)$ be a quadratic form with integer coefficients and p be an odd prime. Let $V = V_Q = V_p$ denote the set of zeros of $Q(\mathbf{x})$ in $\mathbb{Z}_p$ and $|V|$ denotes the cardinality of V. Set $\phi(V_p, \mathbf{y}) = \sum_{\mathbf{x} \in V} e_p(\mathbf{x} \cdot \mathbf{y})$ for $\mathbf{y} \neq \mathbf{0}$ and $\phi(V_p, \mathbf{y}) = |V_p| - p^{n-1}$ for $\mathbf{y} = \mathbf{0}$. In this paper, we give an upper bound for the number of integer solutions of the congruence $Q(\mathbf{x}) \equiv 0 (\text{mod } p)$.

1. Introduction

Let $Q(\mathbf{x}) = Q(x_1, x_2, \ldots, x_n) = \sum_{1 \leqslant i \leqslant j \leqslant n} a_{ij} x_i x_j$ be a quadratic form with integer coefficients in n-variables, and $V = V_p(Q)$ be the algebraic subset of $\mathbb{Z}_p^n$ defined by the equation

2010 Mathematics Subject Classification: 11F11

Keywords and phrases: integral solutions.

Received May 31, 2011

$$Q(\mathbf{x}) \equiv 0 (\bmod\ p), \tag{1}$$

and $\mathcal{B}$ be the box defined by

$$\mathcal{B} = \{\mathbf{x} \in \mathbb{Z}_p^n \,|\, a_i \leqslant x_i < a_i + m_i, 1 \leqslant i \leqslant n\}, \tag{2}$$

where $a_i, m_i \in \mathbb{Z}$, and $0 < m_i < p$ for $1 \leqslant i \leqslant n$. Let $|\mathcal{B}|$ denote the cardinality of the box $\mathcal{B}$. We call the box a cube of size m, if $m_i = m$ for all i. Suppose that n is even and $\det A_Q \not\equiv 0 (\bmod\ p)$, where A_Q is $n \times n$ defining matrix for $Q(\mathbf{x})$. 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 $(. / p)$ denotes the Legendre symbol. Let $Q^*(\mathbf{x})$ be the inverse of the matrix representing $Q(\mathbf{x})$, (mod p). In this paper, we are interested in the following type of problems:

Problem 1. For a box $\mathcal{B}$ with sides of arbitrary lengths, how large must its cardinality be in order to guarantee that $\mathcal{B}$ contains a solution of (1)?

Problem 2. Determine $|\mathcal{B} \cap V_{p,\mathbb{Z}}|$, the number of integer solutions of (1) contained in $\mathcal{B}$?

For addressing these two problems, we shall use Fourier series and exponential sums. We shall obtain

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

$$|\mathcal{B} \cap V_{p,\mathbb{Z}}| \leqslant \begin{cases} 2^n \left(\dfrac{|\mathcal{B}|}{p} + N_{\mathcal{B}} p^{n/2} \right), & \text{if } \Delta = +1, \\ 2^{n+1} \left(\dfrac{|\mathcal{B}|}{p} + N_{\mathcal{B}} p^{n/2} \right), & \text{if } \Delta = -1, \end{cases} \tag{3}$$

where

$$N_{\mathcal{B}} = \prod_{i=1}^{n} \left(\left[\frac{m_i}{p} \right] + 1 \right). \tag{4}$$

If V is the set of zeros of a "nonsingular" quadratic form $Q(\mathbf{x})$, then one can show that

$$|V \cap \mathcal{B}| = \frac{|\mathcal{B}|}{p} + O\left(p^{n/2}(\log p)^n\right), \tag{5}$$

for any box $\mathcal{B}$ (see [2]). It is apparent from (5) that $|V \cap \mathcal{B}|$ is nonempty provided

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

For any $\mathbf{x}, \mathbf{y}$ in $\mathbb{Z}_p^n$, 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 $x \in \mathbb{Z}_p$, let $e_p(x) = e^{2\pi i x/p}$. We use the abbreviation $\sum_{\mathbf{x}} = \sum_{\mathbf{x} \in \mathbb{Z}_p^n}$ for complete sums. The key ingredient in obtaining the identity in (5) is a uniform upper bound on the function

$$\phi(V, \mathbf{y}) = \begin{cases} \displaystyle\sum_{\mathbf{x} \in V} e_p(\mathbf{x} \cdot \mathbf{y}), & \text{for } \mathbf{y} \neq \mathbf{0}, \\ |V| - p^{n-1}, & \text{for } \mathbf{y} = \mathbf{0}. \end{cases} \tag{6}$$

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 $\mathbb{Z}_p^n$ such that $\alpha(\mathbf{x}) \leqslant 0$ 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

$$\alpha(\mathbf{x}) = \sum_{\mathbf{y}} a(\mathbf{y}) e_p(\mathbf{y} \cdot \mathbf{x}),$$

where

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

for all $\mathbf{y} \in \mathbb{Z}_p^n$. Thus

$$\sum_{\mathbf{x} \in V} \alpha(\mathbf{x}) = \sum_{\mathbf{x} \in V} \sum_{\mathbf{y}} a(\mathbf{y}) e_p(\mathbf{y} \cdot \mathbf{x})$$

$$= \sum_{\mathbf{y}} a(\mathbf{y}) \sum_{\mathbf{x} \in V} e_p(\mathbf{y} \cdot \mathbf{x})$$

$$= a(\mathbf{0})|V| + \sum_{\mathbf{y} \neq \mathbf{0}} \alpha(\mathbf{y}) \sum_{\mathbf{x} \in V} e_p(\mathbf{y} \cdot \mathbf{x}).$$

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

$$\sum_{\mathbf{x} \in V} \alpha(\mathbf{x}) = p^{-n}|V| \sum_{\mathbf{x}} \alpha(\mathbf{x}) + \sum_{\mathbf{y} \neq \mathbf{0}} a(\mathbf{y}) \phi(V, \mathbf{y}), \tag{7}$$

where $\phi(V, \mathbf{y})$ is defined by (6). A variation of (7) that is sometimes more useful is

$$\sum_{\mathbf{x} \in V} \alpha(\mathbf{x}) = p^{-1} \sum_{\mathbf{x}} \alpha(\mathbf{x}) + \sum_{\mathbf{y}} a(\mathbf{y}) \phi(V, \mathbf{y}), \tag{8}$$

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

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

$$= p^{n-1} a(\mathbf{0}) + \sum_{\mathbf{y}} a(\mathbf{y}) \phi(V, \mathbf{y}).$$

Equations (7) and (8) 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, $|V| \approx p^{n-1}$ 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 $|V| = p^{n-1} + O(p^n)$ (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 (7) or (8). One tries to make an optimal choice of $\alpha(\mathbf{x})$ in order to minimize the error term. Special cases of (7) and (8) have appeared a number of times in the literature for different types of algebraic sets V; Chalk [1], Tietäväinen [8], and Myerson [7]. The first case treated was to let $\alpha(\mathbf{x})$ be the characteristic function $\chi_S(\mathbf{x})$ of a subset S of $\mathbb{Z}_p^n$, whence (8) gives rise to formulas of the type

$$|V \cap S| = p^{-1}|S| + \text{Error}.$$

Equation (5) is obtained in this manner. Particular attention has been given to the case where $S = \mathcal{B}$, a box of points in $\mathbb{Z}_p^n$. Another popular choice for α is let it be a convolution of two characteristic functions, $\alpha = \chi_S * \chi_T$ for $S, T \subseteq \mathbb{Z}_p^n$. We recall that if $\alpha(\mathbf{x})$ and $\beta(\mathbf{x})$ are complex valued functions defined on $\mathbb{Z}_p^n$, then the convolution of $\alpha(\mathbf{x})$ and $\beta(\mathbf{x})$ 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 $\mathbf{x} \in \mathbb{Z}_p^n$. 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

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

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

$$S_p(Q, \mathbf{y}) = \sum_{\mathbf{x} \in \mathbb{Z}_p^n} e_p(Q(\mathbf{x}) + \mathbf{y} \cdot \mathbf{x}),$$

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

$$\alpha(\mathbf{x}) = \sum_{\mathbf{y}} a(\mathbf{y}) e_p(\mathbf{x} \cdot \mathbf{y}), \quad \beta(\mathbf{x}) = \sum_{\mathbf{y}} b(\mathbf{y}) e_p(\mathbf{x} \cdot \mathbf{y}).$$

Then

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

$$\alpha\beta(\mathbf{x}) = \alpha(\mathbf{x})\beta(\mathbf{x}) = \sum_{\mathbf{y}} (a * b)(\mathbf{y}) e_p(\mathbf{x} \cdot \mathbf{y}), \tag{10}$$

$$\sum_{\mathbf{x}} (\alpha * \beta)(\mathbf{x}) = \left(\sum_{\mathbf{x}} \alpha(\mathbf{x}) \right) \left(\sum_{\mathbf{x}} \beta(\mathbf{x}) \right), \tag{11}$$

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

$$\sum_{\mathbf{y}} |a(\mathbf{y})|^2 = p^{-n} \sum_{\mathbf{x}} |\alpha(\mathbf{x})|^2. \tag{13}$$

The last identity is Parseval's equality.

2. Cochrane's Estimate

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. Consider the congruence

$$Q(\mathbf{x}) \equiv 0 (\text{mod } p).$$

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

Lemma 1 (see, e.g., [3], Lemma 1)**.** *When n is even and* $\Delta = \pm 1$,

$$\phi(V, \mathbf{y}) = \begin{cases} \Delta(p-1)p^{(n/2)-1}, & \text{if } Q^*(\mathbf{y}) = 0, \\ -\Delta p^{(n/2)-1}, & \text{if } Q^*(\mathbf{y}) \neq 0, \end{cases}$$

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

Back to (8), we saw the identity

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

Inserting the value $\phi(V,\, \mathbf{y})$ in Lemma 1 yields (see, e.g., [4]).

Lemma 2 (The fundamental identity). *Suppose* n *is even. For any complex valued* $\alpha(\mathbf{x})$ *on* $\mathbb{Z}_p^n$, *and any quadratic form* $Q(\mathbf{x})$ *with* $\Delta_p(Q) = \pm 1$,

$$\sum_{\mathbf{x}\in V}\alpha(\mathbf{x}) = \underbrace{p^{-1}\sum_{\mathbf{x}}\alpha(\mathbf{x})}_{\textit{main term}} \underbrace{- \Delta\alpha(\mathbf{0})p^{(n/2)-1} + \Delta p^{n/2}\sum_{Q^*(\mathbf{y})=0}a(\mathbf{y})}_{\textit{error terms}}. \tag{14}$$

Let our set $\mathcal{B}$ be a box of points of the type given in (2)

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

and view this box as a subset of $\mathbb{Z}_p^n$ and let $\chi_{\mathcal{B}}$ be its characteristic function with Fourier expansion $\chi_{\mathcal{B}}(\mathbf{x}) = \sum_{\mathbf{y}} a_{\mathcal{B}}(\mathbf{y})e_p(\mathbf{x}\cdot\mathbf{y})$. Then for any $\mathbf{y}\in\mathbb{Z}_p^n$,

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

where the term in the product is taken to be m_i if $y_i = 0$. We apply the fundamental identity with $\alpha(\mathbf{x}) = \chi_{\mathbf{B}_1} * \chi_{\mathbf{B}_2}$ the convolution of $\chi_{\mathbf{B}_1}$, where $\mathbf{B}_1$ and $\mathbf{B}_2$ are boxes such that $\mathbf{B}_1 + \mathbf{B}_2 \subset \mathcal{B}$. Now we have the following two cases:

(1) $\Delta = +1$. In this case, we let $\mathcal{B}$ be centered at origin and take $\mathbf{B}_1 = \mathbf{B}_2 = \frac{1}{2}\mathcal{B}$. Then the coefficients $a(\mathbf{y})$ are positive reals, so the fundamental identity gives us

$$\sum_{\mathbf{x}\in\mathbf{V}} \alpha(\mathbf{x}) > \frac{1}{p}\sum_{\mathbf{x}} \alpha(\mathbf{x}) - \alpha(\mathbf{0})p^{(n/2)-1}$$

$$= \frac{|\mathbf{B}_1|^2}{p} - |\mathbf{B}_1|p^{(n/2)-1}.$$

We see that $\sum_{x\in V}\alpha(x) > 0$, provided $|\mathbf{B}_1| > p^{n/2}$, that is, $|\mathbf{B}| > 2^n p^{n/2}$. Since α is supported on $\mathcal{B}$, we have $\mathcal{B} \cap V \neq \phi$.

(2) $\Delta = -1$. In this case, we need to estimate $\sum_{Q^*(\mathbf{y})=\mathbf{0}} a(\mathbf{y})$, but we do not insist on $\mathcal{B}$ being centered at the origin.

A key tool for estimating the error term $\sum_{Q^*(\mathbf{y})=0} a(\mathbf{y})$ is a good upper bound on $|V \cap \mathcal{B}|$ the number of solutions of (1) with $\mathbf{x} \in \mathcal{B}$. First [5] establishes

Lemma 3 ([5], Lemma 1)**.** *Let S be a closed star-shaped region about the origin in $\mathbb{R}^n$ with $\|\mathbf{x}\| = \max|x_i| < p/2$ for all $\mathbf{x} \in S$.* [*A region of points S in $\mathbb{R}^n$ is said to be star-shaped about the origin*, *if for any point $\mathbf{P}$ in S the line segment joining $\mathbf{P}$ and the origin is contained in S.*] *For $0 < \gamma < 1$, let $\gamma S = \{\gamma\mathbf{x} | \mathbf{x} \in S\}$. Let $V \subseteq \mathbb{Z}^n$ be the set of zeros* mod$p$ *of any form in n-variables over $\mathbb{Z}$. Then*

$$|\gamma S \cap V| \leqslant 1 + \frac{\gamma}{1-\gamma}|S \cap V|.$$

Then using the fundamental identity (14) and Lemma 3, one obtains

Lemma 4 ([5], Lemma 2)**.** *Suppose that $n \geqslant 4$ is even, $\Delta_p(Q) = -1$ and $V = V_p(Q)$. Let $\mathcal{B}$ be a box of points of the type*

$$\mathcal{B} = \{\mathbf{y} \in \mathbb{Z}_p^n \mid |y_i| \leqslant \beta_i,\ 1 \leqslant i \leqslant n\},$$

for some nonnegative integers $\beta_i < p/2$, $1 \leqslant i \leqslant n$. *Let t be a given positive integer. If* $\beta_i < 2^{-n-3-t}p$, *for* $1 \leqslant i \leqslant n$, *or* $|\mathcal{B}| > 2^{-n^2-2n-tn}p^{n/2}$, *then*

$$|\mathcal{B} \cap V| \leqslant 2^{n^2+(3+t)n+1}\frac{|\mathcal{B}|}{p} + \frac{1}{2^t}p^{(n/2)-1}.$$

A second appeal to the fundamental identity yields

Lemma 5 ([5], Theorem 2)**.** *Suppose that* $n \geqslant 4$ *is even,* $p \geqslant 2^{4n+6}10^{2n-2}$ *and that* $\Delta_p(Q) = -1$. *If* $m_i \geqslant 2^{5n+7}10^n$ *for* $1 \leqslant i \leqslant n$, *and* $|\mathcal{B}| > 2^{3n^2+4n+2}10^n p^{n/2}$, *then* $\mathcal{B}$ *contains a nonzero solution of* (1).

3. Proof of Theorem 1 when $\Delta = +1$

Let $\mathcal{B}$ be the box of points in $\mathbb{Z}^n$ given by (2)

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

where $m_i = q_i p + r_i$, $0 \leqslant r_i < p$, and $q_i, r_i \in \mathbb{Z}$. Thus, the number of points in $\mathcal{B}$ (cardinality of $\mathcal{B}$) is $|\mathcal{B}| = \prod_{i=1}^n m_i$. As we mentioned before our interest in this paper is determining the number of integral solutions of

$$Q(\mathbf{x}) \equiv 0 (\mathrm{mod}\ p),$$

with $x \in \mathcal{B}$. First, we treat the case where all $m_i \leqslant p$. In this case, we can view the box $\mathcal{B}$ in (2) as a subset of $\mathbb{Z}_p^n$ and let $\chi_{\mathcal{B}}$ be its characteristic function with Fourier expansion $\chi_{\mathcal{B}}(\mathbf{x}) = \sum_{\mathbf{y}} a_{\mathcal{B}}(\mathbf{y}) e_p(\mathbf{x} \cdot \mathbf{y})$. Then for any $\mathbf{y} \in \mathbb{Z}_p^n$,

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

Lemma 6. *Let $\mathcal{B}$ be a box of type* (1) *centered at the origin with all $m_i \leqslant p$, and $V_p = V_p(Q)$ denote to the set of solutions of* (1) *in $\mathbb{Z}_p^n$. If $\Delta_Q = +1$, then*

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

Proof. Since $\Delta_Q = +1$, the fundamental identity (modulo p) is

$$\sum_{\mathbf{x} \in V_p} \alpha(\mathbf{x}) = p^{-1}\sum_{\mathbf{x}} \alpha(\mathbf{x}) - \alpha(\mathbf{0})p^{(n/2)-1} + p^{n/2} \sum_{Q^*(\mathbf{y})=0} a(\mathbf{y}), \tag{15}$$

by Lemma 2. Set $\alpha = \chi_{\mathcal{B}} * \chi_{\mathcal{B}}$, the convolution of $\chi_{\mathcal{B}}$ with itself, i.e.,

$$\begin{aligned}
\alpha(\mathbf{x}) &= \sum_{\mathbf{u}} \chi_{\mathcal{B}}(\mathbf{u})\chi_{\mathcal{B}}(\mathbf{x} - \mathbf{u}) \\
&= \sum_{\mathbf{u}+\mathbf{v}=\mathbf{x}} \chi_{\mathcal{B}}(\mathbf{u})\chi_{\mathcal{B}}(\mathbf{v}) \\
&= \sum_{\mathbf{u}}\sum_{\mathbf{y}} a_{\mathcal{B}}(\mathbf{y})e_p(\mathbf{u} \cdot \mathbf{y})\sum_{\mathbf{z}} a_{\mathcal{B}}(\mathbf{z})e_p(\mathbf{z} \cdot (\mathbf{x} - \mathbf{u})) \\
&= \sum_{\mathbf{y}}\sum_{\mathbf{z}} a_{\mathcal{B}}(\mathbf{y})a_{\mathcal{B}}(\mathbf{z})e_p(\mathbf{z} \cdot \mathbf{x})\sum_{\mathbf{u}} e_p(\mathbf{u} \cdot (\mathbf{y} - \mathbf{z})) \\
&= p^n \sum_{\mathbf{y}} a_{\mathcal{B}}^2(\mathbf{y})e_p(\mathbf{y} \cdot \mathbf{x}),
\end{aligned}$$

so that the Fourier coefficients $a(\mathbf{y})$ of $\alpha(\mathbf{x})$ are $p^n a_{\mathcal{B}}^2(\mathbf{y})$. Since $\mathcal{B}$ is centered at the origin of the Fourier coefficients $a_{\mathcal{B}}(\mathbf{y})$ are all real. Thus the coefficients $a(\mathbf{y})$ of $\chi_{\mathcal{B}} * \chi_{\mathcal{B}}$ are all positive. By using Parseval's identity (13),

$$\sum_{\mathbf{y}} |a(\mathbf{y})| = p^n \sum_{\mathbf{y}} |a_{\mathcal{B}}(\mathbf{y})|^2 = \sum_{\mathbf{y}} \chi_{\mathcal{B}}^2(\mathbf{y}) = |\mathcal{B}|. \tag{16}$$

Next by (15), we observe that

$$\sum_{\mathbf{x}\in V_p} \alpha(\mathbf{x}) \leqslant p^{-1}\sum_{\mathbf{x}} \alpha(\mathbf{x}) + p^{n/2}\sum_{\mathbf{y}} a(\mathbf{y})$$

$$= p^{-1}\sum_{\mathbf{x}} (\chi_{\mathcal{B}} * \chi_{\mathcal{B}})(\mathbf{x}) + p^{n/2}\sum_{\mathbf{y}} |\alpha(\mathbf{y})|.$$

Then, using the identity (12) and (16), the above is

$$\sum_{\mathbf{x}\in V_p} \alpha(\mathbf{x}) \leqslant p^{-1}\left[\left(\sum_{\mathbf{u}} \chi_{\mathcal{B}}(\mathbf{u})\right)\cdot\left(\sum_{\mathbf{v}} \chi_{\mathcal{B}}(\mathbf{v})\right)\right] + p^{n/2}|\mathcal{B}|$$

$$= p^{-1}|\mathcal{B}||\mathcal{B}| + p^{n/2}|\mathcal{B}|$$

$$= \frac{|\mathcal{B}|^2}{p} + p^{n/2}|\mathcal{B}|. \tag{17}$$

On the other hand, for any $\mathbf{x} \in \mathcal{B}$, we claim that

$$\alpha(\mathbf{x}) = \chi_{\mathcal{B}} * \chi_{\mathcal{B}}(\mathbf{x}) \geqslant 2^{-n}|\mathcal{B}|. \tag{18}$$

To see this, we shall argue as follows. Let $I = [-M, M]$ be an interval symmetric about 0. We need first to prove that for $x \in I$,

$$\chi_I * \chi_I(x) \geqslant \frac{1}{2}|I| = \frac{1}{2}(2M + 1). \tag{19}$$

To this end, we have to count the number of points $(u, v) \in I \times I$ such that $u + v = x$. We have two cases. If $-M \leqslant x \leqslant 0$, then the number of points is $2M + x + 1$, specifically $x = u + (x - u), -M \leqslant u \leqslant x + M$. Thus plainly the total number of the points is greater than or equal to

$$2M - M + 1 = M + 1 \geqslant \frac{1}{2}|I|.$$

If $0 < x \leqslant M$, then we have $2M - x + 1$ points, specifically $x = u + (x - u)$, $x - M \leqslant u \leqslant M$, and thus once again the total number of the points is greater than or equal to

$$2M - M + 1 = M + 1 \geqslant \frac{1}{2}|I|.$$

The two cases imply (19). Thus, it follows immediately by (19), that for $x \in I_1 \times \ldots \times I_n = \mathcal{B}$,

$$\alpha(\mathbf{x}) = \prod_{i=1}^{n} \chi_{I_i} * \chi_{I_i}(\mathbf{x}) \geqslant \prod_{i=1}^{n} \frac{1}{2}|I_i| = 2^{-n}|\mathcal{B}|,$$

which is (18). Now we return to complete proving the lemma. From (18), it follows that

$$\sum_{\mathbf{x} \in V_p} \alpha(\mathbf{x}) \geqslant \sum_{\mathbf{x} \in V_p \cap \mathcal{B}} 2^{-n}|\mathcal{B}| = 2^{-n}|\mathcal{B}|\,|\mathcal{B} \cap V_p|. \tag{20}$$

Thus, putting (17) and (20) together and simplifying, we conclude that

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

The lemma is thereby proved. □

Lemma 6 is stated for boxes centered at the origin. In the next lemma, we will drop this hypothesis and prove the lemma for arbitrary boxes. We will get the same result.

Lemma 7. *Let* $\mathcal{B}$ *be any box of type* (2) *with all* $m_i \leqslant p$ *and* $V_p = V_p(Q)$ *denote to the set of solutions of* (1) *in* $\mathbb{Z}_p^n$. *If* $\Delta_Q = +1$, *then*

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

Proof. Again as $\Delta_Q = +1$, the fundamental identity (modulo p) is as (15)

$$\sum_{\mathbf{x} \in V_p} \alpha(\mathbf{x}) = p^{-1} \sum_{\mathbf{x}} \alpha(\mathbf{x}) - \alpha(\mathbf{0}) p^{(n/2)-1} + p^{n/2} \sum_{Q^*(\mathbf{y})=0} a(\mathbf{y}).$$

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

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

Then

$$\sum_{\mathbf{x}} \alpha(\mathbf{x}) = |\mathcal{B}|\,|\mathcal{B}'| = |\mathcal{B}|^2, \tag{21}$$

$$\alpha(0) = \sum_{\substack{u\in\mathcal{B} \\ \mathbf{u}+\mathbf{v}=\mathbf{0}}} \sum_{v\in\mathcal{B}'} 1 \leqslant |\mathcal{B}|, \tag{22}$$

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

Thus, using the Cauchy-Schwartz inequality (see, e.g., [6]) and Parseval's identity (13), we obtain

$$\begin{aligned} \sum_{\mathbf{y}} |a(\mathbf{y})| &= p^n \sum_{\mathbf{y}} |a_{\mathcal{B}}(\mathbf{y}) a_{\mathcal{B}'}(\mathbf{y})| \\ &\leqslant p^n \left(\sum_{\mathbf{y}} |a_{\mathcal{B}}(\mathbf{y})|^2\right)^{1/2} \left(\sum_{\mathbf{y}'} |a_{\mathcal{B}'}(\mathbf{y}')|^2\right)^{1/2} \\ &\leqslant p^n \left(\frac{1}{p^n} \sum_{\mathbf{y}} \chi^2_{\mathcal{B}}(\mathbf{x})\right)^{1/2} \left(\frac{1}{p^n} \sum_{\mathbf{y}} \chi^2_{\mathcal{B}'}(\mathbf{x})\right)^{1/2} \\ &= |\mathcal{B}|^{1/2} |\mathcal{B}'|^{1/2} = |\mathcal{B}|. \end{aligned} \tag{23}$$

Thus, by the fundamental identity (15) and (21), (22), (23), if $\Delta = +1$,

$$\begin{aligned} \sum_{\mathbf{x}\in V_p} \alpha(\mathbf{x}) &\leqslant p^{-1} \sum_{\mathbf{x}} \alpha(\mathbf{x}) + p^{n/2} \sum_{\substack{\mathbf{y} \\ Q^*(\mathbf{y})=0}} |a(\mathbf{y})| \\ &\leqslant p^{-1} \sum_{\mathbf{x}} \alpha(\mathbf{x}) + p^{n/2} \sum_{\mathbf{y}} |a(\mathbf{y})| \\ &\leqslant \frac{|\mathcal{B}|^2}{p} + p^{n/2} |\mathcal{B}|. \end{aligned} \tag{24}$$

Now we claim that

$$\sum_{\mathbf{x}\in V_p} \alpha(\mathbf{x}) \geqslant \sum_{\mathbf{x}\in V_p \cap \mathcal{B}} 2^{-n}|\mathcal{B}| = 2^{-n}|\mathcal{B}|\,|V_p \cap \mathcal{B}|. \tag{25}$$

To see (25), we are going to argue as follows. Let

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

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

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

Thus for any $x \in I$,

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

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

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

Hence for any $x \in I$,

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

So

$$\alpha(\mathbf{x}) = \chi_{\mathcal{B}} * \chi_{\mathcal{B}'}(\mathbf{x}) \geqslant 2^{-n}|\mathcal{B}|,$$

and the claim follows. Now we combine (24) and (25), we get

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

which completes the proof of Lemma 7. □

Next we consider larger boxes, where the m_i may exceed p. Let $N_{\mathcal{B}}$ as given by (4)

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

Proof of Theorem 1 when $\Delta = +1$**.** Partition $\mathcal{B}$ 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 $\leqslant p$. Thus Lemma 7 can be applied to each B_i. We obtain

$$\begin{aligned} |\mathcal{B} \cap V_{p,\mathbb{Z}}| &= \sum_{i=1}^{N} |B_i \cap V_p| \\ &\leqslant \sum_{i=1}^{N} 2^n\left(\frac{|B_i|}{p} + p^{n/2}\right) \\ &= \frac{2^n}{p}\sum_{i=1}^{N}|B_i| + N2^n p^{n/2} \\ &= 2^n\left(\frac{|\mathcal{B}|}{p} + Np^{n/2}\right). \end{aligned}$$

So the proof of (3) when $\Delta = +1$ is complete.

4. Proof of Theorem 1 when $\Delta = -1$

We start by noticing that Lemma 7 could be rewritten in this case as follows:

Lemma 8. *Let* $\mathcal{B}$ *be any box of type* (2) *with all* $m_i \leqslant p$, *and* $V_p = V_p(Q)$ *denote to the set of solutions of* (1) *in* $\mathbb{Z}_p^n$. *If* $\Delta_p = -1$, *then*

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

Proof. The proof is similar to the proof of Lemma 7. The fundamental identity modulo p when $\Delta_p = -1$ is given by

$$\sum_{\mathbf{x}\in V_p} \alpha(\mathbf{x}) = p^{-1}\sum_{\mathbf{x}} \alpha(\mathbf{x}) + \alpha(\mathbf{0})p^{(n/2)-1} - p^{n/2}\sum_{Q^*(\mathbf{y})=0} a(\mathbf{y}). \tag{26}$$

Let α be as given in the proof of Lemma 7. By (26), (21), (22), and (23), we have

$$\sum_{\mathbf{x}\in V_p} \alpha(\mathbf{x}) \leqslant \frac{|\mathcal{B}|^2}{p} + p^{(n/2)-1}|\mathcal{B}| + p^{n/2}\sum_{\mathbf{y}}|a(\mathbf{y})|$$

$$\leqslant \frac{|\mathcal{B}|^2}{p} + p^{n/2}|\mathcal{B}|\left(\frac{1}{p} + 1\right)$$

$$\leqslant \frac{|\mathcal{B}|^2}{p} + 2p^{n/2}|\mathcal{B}|.$$

But, in the proof of Lemma 7, we proved that

$$\sum_{\mathbf{x}\in V_p} \alpha(\mathbf{x}) \geqslant \sum_{\mathbf{x}\in V_p\cap\mathcal{B}} 2^{-n}|\mathcal{B}| = 2^{-n}|\mathcal{B}|\,|\mathcal{B}\cap V_p|.$$

Thus, it follows

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

which is the assertion of the lemma. □

Proof of Theorem 1 when $\Delta = -1$. We proceed just as in the proof of the case $\Delta = +1$. Partition $\mathcal{B}$ into $N = N_{\mathcal{B}}$ smaller boxes B_i. This means

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

where each B_i has all of its edge lengths $\leqslant p$. Apply Lemma 8 to each $\mathcal{B}_i$, we thus obtain

$$\begin{aligned}|\mathcal{B} \cap V_{p,\mathbb{Z}}| &= \sum_{i=1}^{N} |B_i \cap V_p| \\ &\leqslant \sum_{i=1}^{N} 2^{n+1}\left(\frac{|B_i|}{p} + p^{n/2}\right) \\ &= \frac{2^{n+1}}{p}\sum_{i=1}^{N}|B_i| + N2^n p^{n/2} \\ &= 2^{n+1}\left(\frac{|\mathcal{B}|}{p} + Np^{n/2}\right),\end{aligned}$$

finishing the proof of (3).

References

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

[2] T. Cochrane, Small Solutions of Congruences, PhD Thesis, University of Michigan, 1984.

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

[4] T. Cochrane, Small zeros of quadratic forms modulo p, II, Proceedings of the IIinois Number Theory Conference, (1989), Birkhauser, Boston, (1990), 91-94.

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

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

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

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

■