SMALL ZEROS OF QUADRATIC CONGRUENCES TO A PRIME POWER MODULUS

by

ALI HAFIZ MAWDAH HAKAMI

B.S., King Abdulaziz University, Saudi Arabia, 1996
M.S., Kansas State University, U.S.A., 2004

AN ABSTRACT OF A DISSERTATION

submitted in partial fulfillment of
the requirements for the degree

DOCTOR OF PHILOSOPHY

Department of Mathematics
College of Arts and Sciences

KANSAS STATE UNIVERSITY
Manhattan, Kansas

2009

ABSTRACT

Let m be a positive integer, p be an odd prime, and $\mathbb{Z}_{p^m} = \mathbb{Z}/(p^m)$ be the ring of integers modulo p^m. Let

$$Q(\mathbf{x}) = Q(x_1, x_2, ..., x_n) = \sum_{1 \le i \le j \le n} a_{ij} x_i x_j \,,$$

be a quadratic form with integer coefficients. Suppose that n is even and $\det A_Q \not\equiv 0 \pmod{p}$. Set $\Delta = ((-1)^{n/2} \det A_Q \,/\, p)$, where $(\cdot / p)$ is the Legendre symbol and $\|\mathbf{x}\| = \max |x_i|$. Let V be the set of solutions the congruence

$$Q(\mathbf{x}) \equiv 0 \pmod{p^m}, \qquad (\#)$$

contained in $\mathbb{Z}^n$ and let $\mathscr{B}$ be any box of points in $\mathbb{Z}^n$ of the type

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

where $a_i, m_i \in \mathbb{Z}, 1 \le m_i \le p^m$.

In this dissertation we use the method of exponential sums to investigate how large the cardinality of the box $\mathscr{B}$ must be in order to guarantee that there exists a solution $\mathbf{x}$ of $(\#)$ in $\mathscr{B}$. In particular we will focus on cubes (all m_i equal) centered at the origin in order to obtain primitive solutions with $\|\mathbf{x}\|$ small. For $m = 2$ and $n \ge 4$ we obtain a primitive solution with $\|\mathbf{x}\| \le \max\left\{2^5 p, 2^{18}\right\}$. For $m = 3$, $n \ge 6$, and $\Delta = +1$, we get $\|\mathbf{x}\| \le \max\left\{2^{2/n} p^{(3/2)+(3/n)}, 2^{(2n+4)/(n-2)}\right\}$. Finally for any $m \ge 2$, $n \ge m$, and any nonsingular quadratic form we obtain $\|\mathbf{x}\| \le \max\{6^{1/n} p^{m[(1/2)+(1/n)]}, 2^{2(n+1)/(n-2)} 3^{2/(n-2)}\}$.

Others results are obtained for boxes $\mathscr{B}$ with sides of arbitrary lengths.

SMALL ZEROS OF QUADRATIC CONGRUENCES TO A PRIME POWER MODULUS

by

ALI HAFIZ MAWDAH HAKAMI

B.S., King Abdulaziz University, Saudi Arabia, 1996
M.S., Kansas State University, U.S.A., 2004

A DISSERTATION

submitted in partial fulfillment of
the requirements for the degree

DOCTOR OF PHILOSOPHY

Department of Mathematics
College of Arts and Sciences

KANSAS STATE UNIVERSITY
Manhattan, Kansas

2009

Approved by:

Major Professor
Todd Cochrane

Copyright

ABSTRACT

Let m be a positive integer, p be an odd prime, and $\mathbb{Z}_{p^m} = \mathbb{Z}/(p^m)$ be the ring of integers modulo p^m. Let

$$Q(\mathbf{x}) = Q(x_1, x_2, ..., x_n) = \sum_{1 \le i \le j \le n} a_{ij} x_i x_j \,,$$

be a quadratic form with integer coefficients. Suppose that n is even and $\det A_Q \not\equiv 0 \pmod{p}$. Set $\Delta = ((-1)^{n/2} \det A_Q \,/\, p)$, where $(\cdot / p)$ is the Legendre symbol and $\|\mathbf{x}\| = \max |x_i|$. Let V be the set of solutions the congruence

$$Q(\mathbf{x}) \equiv 0 \pmod{p^m}, \qquad (\#)$$

contained in $\mathbb{Z}^n$ and let $\mathscr{B}$ be any box of points in $\mathbb{Z}^n$ of the type

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

where $a_i, m_i \in \mathbb{Z}, 1 \le m_i \le p^m$.

In this dissertation we use the method of exponential sums to investigate how large the cardinality of the box $\mathscr{B}$ must be in order to guarantee that there exists a solution $\mathbf{x}$ of $(\#)$ in $\mathscr{B}$. In particular we will focus on cubes (all m_i equal) centered at the origin in order to obtain primitive solutions with $\|\mathbf{x}\|$ small. For $m = 2$ and $n \ge 4$ we obtain a primitive solution with $\|\mathbf{x}\| \le \max\left\{2^5 p, 2^{18}\right\}$. For $m = 3$, $n \ge 6$, and $\Delta = +1$, we get $\|\mathbf{x}\| \le \max\left\{2^{2/n} p^{(3/2)+(3/n)}, 2^{(2n+4)/(n-2)}\right\}$. Finally for any $m \ge 2$, $n \ge m$, and any nonsingular quadratic form we obtain $\|\mathbf{x}\| \le \max\{6^{1/n} p^{m[(1/2)+(1/n)]}, 2^{2(n+1)/(n-2)} 3^{2/(n-2)}\}$.

Others results are obtained for boxes $\mathscr{B}$ with sides of arbitrary lengths.

TABLE OF CONTENTS

LIST OF FIGURES

ACKNOWLEDGMENTS

All praise to Almighty Allah the most gracious and merciful by whose grace this research has been completed.

First, I am deeply indebted to my advisor, **Professor Todd Cochrane,** for his advice, encouragement and guidance. He re-read many versions of this thesis, and every other research paper I have written to date, and provided me with countless hours of his time. I consider myself very fortunate to have had him as my advisor. He has had many students, and all that I have spoken to are in agreement that he is a phenomenal advisor. It is humbling to know that we can never possibly equal him. He motivates his students to work hard and to go farther than they ever thought they were capable of. We can only try to emulate him.

I would like to thank the members of my committee. To Professor Christopher Pinner for his support, for the many valuable discussions and for his comments on the writing of this dissertation. I would also like to thank Professor Andrew Bennett who was instrumental in getting me to this point. Many thanks to Professor David Allen for his interest in my work. I would also like to thank Professor William Dunn for serving as chair for my final exam.

I want to express special thanks to the Department of Mathematics at Kansas State University, and especially to Professor Louis Pigno, the Department Head who gave me the right leads and advice and for helping me throughout my stay here.

I cannot help but mention how thankful I am to the present Director of Graduate Studies, Professor David Yetter, the Graduate Studies Secretary Hannah Davenport, and others for their friendship, encouragement and strong support.

I want to thank my family for believing in me and supporting me throughout my work in particular my wife, Eman, for being my better half. Also I want to express my thanks and appreciation to my brothers for all they have done for me including help, support, and patience during my long journey of study.

I have to apologize to my sons Halah and Ibraheem for having deprived them of time which normally would have been devoted to them and to family life.

I would like to thank King Khalid University in Saudi Arabia for providing financial support throughout my graduate studies. The thanks extend to all the people who have helped me during my study in the United States, especially the people in the Saudi Cultural Mission to the USA.

A special thanks go to my brother **Dr. Abdullah Alwalidi** (Director of e-learning Center - King Khalid University) for the real friendship and support I received from him during all the time I spent in the USA.

Last, but not least, I wish give a special thank you to the two people who have stood behind me as a source of unwavering support, my Mom and Dad.

DEDICATION

To my loving parents, my wife, my children, and my brothers.... I could not have completed my study without their love, support and encouragement....

Introduction and Definitions

The main purpose of this thesis is to find small primitive solutions of a quadratic congruence modulo p^m, $m \geq 2$. The historical background of this subject is given in §0.2 below, but first we give the definition of a small primitive solution of quadratic form modulo a positive integer M.

§0.1. Definition of "small primitive solution" of a quadratic form modulo M.

Let

$$Q(\mathbf{x}) = Q(x_1, x_2, ..., x_n) = \sum_{1 \leq i \leq j \leq n} a_{ij} x_i x_j \,,$$

be a quadratic form over $\mathbb{Z}$ and M be a positive integer. Consider the congruence

$$Q(\mathbf{x}) \equiv 0 \pmod{M}. \tag{0.1}$$

By the norm of a point $\mathbf{x}$ we mean $\|\mathbf{x}\| = \max_i |x_i|$ and by "small solution" we mean a nonzero integral solution $\mathbf{x}$ of (0.1) such that $\|\mathbf{x}\| < M^\delta$ for some positive constant $\delta < 1$. The constant δ may depend on n, but not on M. Our interest is in finding a primitive solution of (0.1), a solution $\mathbf{x}$ with $\gcd(x_1, ..., x_n, M) = 1$, that is, for any prime divisor p of M, $p \nmid x_i$ for some i.

***Example*:** Let $Q(\mathbf{x}) = x_1^2 + \cdots + x_n^2$. Then it is clear that any nonzero solution $\mathbf{x}$ of (0.1) 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.

Our interest is in primitive solutions to rule out trivial small solutions such as $(p,p,...,p)$ with $M=p^2$.

§0.2. Historical background.

Let $Q(\mathbf{x})=Q(x_1,...,x_n)$ be a quadratic form over $\mathbb{Z}$ and M be any positive integer. As we mentioned we are looking for nontrivial solutions of (0.1) with $\|\mathbf{x}\|<M^{\delta}$ for some $\delta\geq 1/2$.

Schinzel, Schlickewi and Schmidt (1971, [**17**]) proved that (0.1) has a nonzero solution with $\|\mathbf{x}\|< M^{(1/2)+1/2(n-1)}$ for $n\geq 3$. Thus for any $\varepsilon>0$ we get a nonzero solution of (0.1) with $\|\mathbf{x}\|<M^{1/2+\varepsilon}$ provided n is sufficiently large. We note that the solution obtained by their method is not necessarily a primitive solution. Indeed, when $M=p^2$ they use the trivial solution $(p,0,0,...,0)$.

Now let $M=p$, with p an odd prime, and consider finding small solutions to the quadratic congruence

$$Q(\mathbf{x})\equiv 0 \pmod{p}. \tag{0.2}$$

Heath-Brown (1985, [**15**]) obtained a nonzero solution of (0.2) with $\|\mathbf{x}\|\ll p^{1/2}\log p$ for $n\geq 4$. (That is $\|\mathbf{x}\|< C\,p^{1/2}\log p$ for some constant C). His result was an improvement on the result of [**17**] in this case. Wang Yuan (1988, [**18**]) generalized Heath-Brown's work to all finite fields.

Cochrane (1990, [**8**]) improved this to $\|\mathbf{x}\|<\max\left\{2^{19}p^{1/2},2^{22}10^6\right\}$. That is $\|\mathbf{x}\|\ll \sqrt{p}$. In many special cases, it is known that there exists a nonzero solution of (0.2) with $\|\mathbf{x}\|< p^{1/2}$, for instance, when $\Delta_p(Q)=0$ or 1 (1987, [**4**]). Here $\Delta_p(Q)$ is defined as following

$$\Delta_p(Q)=\begin{cases}\left((-1)^{n/2}\det Q/p\right) & \text{if} \quad p\nmid \det Q,\\ 0 & \text{if} \quad p\,\Big|\,\det Q,\end{cases}$$

where $(\cdot / p)$ denotes the Legendre symbol and $\det Q$ is the determinant of the matrix representing Q; see section 1.6. We also get $\|\mathbf{x}\| < p^{1/2}$ when Q is of the form $Q_1(x_1, x_2) + Q_2(x_3, x_4)$ (1989, Cochrane [**5**]), and when Q is any quadratic form with $n > 4\log_2 p + 3$ (1989, Cochrane [**5**]). Wang Yuan (1989, [**19**]) once more has generalized Cochrane's work, to arbitrary finite fields.

If $M = pq$, a product of two distinct primes, we are seeking a solution of the congruence,

$$Q(\mathbf{x}) \equiv 0 \pmod{pq}.$$

We find:

Heath-Brown (1991, [**16**]): $\|\mathbf{x}\| \ll M^{1/2+\varepsilon}$, for $n > 4$ and $\varepsilon > 0$.

Cochrane (1995, [**10**]): $\|\mathbf{x}\| \ll M^{1/2}$, for $n > 4$. Again this result sharpened the result of Heath-Brown.

§0.3. Thesis organization and statement of results.

The outline of this thesis is as follows. In Chapter 1 we study briefly the distribution of solutions to quadratic forms over $\mathbb{Z}_p$ and give the basic tools that we need for our work. In addition, we concentrate on the key ideas of the technique of Cochrane for finding a small solution of (0.2), which amounts to finding integral solutions contained in a small box centered about the origin. We give a small improvement of the constant in his estimate.

Theorem 0.1: [Theorem 1.3, p 12] *For any quadratic form* $Q(\mathbf{x})$ *with* $n \geq 4$ *and any prime* p, *there exists a primitive solution* $\mathbf{x}$ *of* (0.2) *with* $\|\mathbf{x}\| < \min\left\{p^{2/3}, 2^{19} p^{1/2}\right\}$.

At the end of this chapter we give a quick look at exponential sums and the diagonalization of a quadratic form over $\mathbb{Z}_{p^m}$.

In Chapter 2 we generalize $(\mathrm{mod}\, p)$ methods for obtaining a small primitive solution of the congruence

$$Q(\mathbf{x}) \equiv 0 \pmod{p^2}. \tag{0.3}$$

We show:

Theorem 0.2 [Theorem 2.1, p 24] *For any odd prime p and nonsingular quadratic form $Q(\mathbf{x})$ with $n \geq 4$, there exists a primitive solution of* (0.3) *with*

$$\|\mathrm{x}\| \leq \begin{cases} \max\left\{2^5 p, 2^{18}\right\} & \textit{for } \Delta = +1, \\ \max\left\{2^5 p, 2^9\right\} & \textit{for } \Delta = -1. \end{cases}$$

Note that this bound is best possible (order $(p^2)^{1/2}$) up to a constant.

In Chapter 3, we study the congruence

$$Q(\mathbf{x}) \equiv 0 \pmod{p^3}. \tag{0.4}$$

We prove:

Theorem 0.3 [Theorem 3.5, p 86] *For any quadratic form $Q(\mathbf{x})$ with $n \geq 4$ and any odd prime p, there exists a primitive solution of* (0.4) *with*

$$\|\mathrm{x}\| \leq \begin{cases} \max\left\{2^7 p^{3/2}, 2^{38}\right\} & \textit{for } \Delta = +1, \\ \max\left\{2^{2/n} p^{(3/2)+(3/n)}, 2^{(2n+4)/(n-2)}\right\} & \textit{for } \Delta = -1. \end{cases}$$

When $\Delta = 1$, we have a best possible type bound.

Finally, in Chapter 4, we address the question of finding small solutions of

$$Q(\mathbf{x}) \equiv 0 \pmod{p^m}, \tag{0.5}$$

for arbitrary prime powers p^m. We establish:

Theorem 0.4 [Theorem 4.1, p 88] *For any quadratic form $Q(\mathbf{x})$ with $n \geq 4$ and any odd prime p, there exists a primitive solution of* (0.5) *with* $\|\mathbf{x}\| \leq \max\{6^{1/n} p^{m[(1/2)+(1/n)]}, 2^{2(n+1)/(n-2)} 3^{2/(n-2)}\}$.

Chapter 1

Preliminaries

In this research we shall follow closely the method of Cochrane [**8**] for finding small zeros of quadratic forms modulo p. Thus we shall give a summary of the key ideas of that method. In the following sections we shall establish analogous results but for modulo p^m, $m \geq 2$. Also we will give a small improvement of his result for mod p (see Theorem 1.3 in this chapter).

§1.1 A brief study of quadratic forms over the finite field $\mathbb{Z}_p$.

The aim of this section is to review the most important concepts that will be needed in our work, on the distribution of zeros of a quadratic form over $\mathbb{Z}_p$ the finite field in p elements, where p is a prime. For more details the reader is referred to [**2**], [**26**], [**27**].

1.1.1. Overview.

Let

$$Q(\mathbf{x}) = Q(x_1, x_2, ..., x_n) = \sum_{1 \leq i \leq j \leq n} a_{ij} x_i x_j \,,$$

be a quadratic form with integer coefficients in n-variables, $V = V_p(Q)$ the algebraic subset of $\mathbb{Z}_p^n$ defined by the equation $Q(\mathbf{x}) = 0$. Our interest is in the problem of finding points in V with the variables restricted to

a box of the type

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

where $a_i, m_i \in \mathbb{Z}$, and $0 < m_i < p$ for $1 \le i \le n$. (Here we have identified $\mathbb{Z}_p$ with the set of integers $\{0, 1, \ldots, p-1\}$).

If V is the set of zeros of a "nonsingular" Quadratic form $Q(\mathbf{x})$ (see §1.5), then one can show that

$$|V \bigcap \mathscr{B}| = \frac{|\mathscr{B}|}{p} + O\left(p^{n/2} (\log p)^{mn}\right), \tag{1.1}$$

for any box $\mathscr{B}$ where the brackets $||$ are used to denote the cardinality of the set inside the brackets (see [**1**]). It is apparent from (1.1) that $|V \bigcap \mathscr{B}|$ is nonempty provided

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

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 (1.1) is a uniform upper bound on the function

$$\phi(V, \mathbf{y}) = \begin{cases} \sum\limits_{\mathbf{x} \in V} e_p(\mathbf{x} \cdot \mathbf{y}) & \text{for} \quad \mathbf{y} \neq \mathbf{0}, \\ |V| - p^{n-1} & \text{for} \quad \mathbf{y} = \mathbf{0}. \end{cases} \tag{1.2}$$

1.1.2. Method of proof.

In order to show that $\mathscr{B} \bigcap V$ is nonempty we can proceed as follows. Let $\alpha(\mathbf{x})$ be a real valued function on $\mathbb{Z}_p^n$ such that $\alpha(\mathbf{x}) \le 0$ for all $\mathbf{x}$ not in $\mathscr{B}$. If we can show that $\sum_{\mathbf{x} \in V} \alpha(\mathbf{x}) > 0$ then it will follow that $\mathscr{B} \bigcap V$ 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

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

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

$$\sum_{\mathbf{x}\in V}\alpha(\mathbf{x}) = p^{-n}|V|\sum_{\mathbf{x}}\alpha(\mathbf{x}) + \sum_{\mathbf{y}\neq\mathbf{0}} a(\mathbf{y})\,\phi(V,\mathbf{y}), \tag{1.3}$$

where $\phi(V,\mathbf{y})$ is defined by (1.2). A variation of (1.3) that is sometimes more useful is

$$\sum_{\mathbf{x}\in V}\alpha(\mathbf{x}) = p^{-1}\sum_{\mathbf{x}}\alpha(\mathbf{x}) + \sum_{\mathbf{y}} a(\mathbf{y})\,\phi(V,\mathbf{y}), \tag{1.4}$$

which is obtained from (1.3) by noticing that $|V| = \phi(V,\mathbf{0}) + p^{n-1}$, whence

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

Equation (1.3) and (1.4) 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 $|V| = p^{n-1} + O(p^{n/2})$. (That is $\left|\phi(V,\mathbf{0})\right| \ll p^{n/2}$).

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 (1.3) or (1.4). One tries to make an optimal choice of $\alpha(\mathbf{x})$ in order to minimize the error term. Special cases of (1.3) and (1.4) have appeared a number of times in the literature for different types of algebraic sets V; Chalk [**22**], Tietäväinen [**24**], and Myerson [**23**]. 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 (1.4) gives rise to formulas of the type

$$|V \bigcap S| = p^{-1}|S| + Error. \tag{1.5}$$

Equation (1.1) is obtained in this manner. Particular attention has been given to the case where $S = \mathscr{B}$, a box of points in $\mathbb{Z}_p^n$. Another popular choice for α is let it be a convolution of two characteristic function, $\alpha = \chi_S * \chi_T$ for $S,T \subseteq \mathbb{Z}_p^n$. We recall that if $\alpha(\mathbf{x})$, $\beta(\mathbf{x})$ are complex valued functions defined on $\mathbb{Z}_p^n$ 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 $\mathbf{x} \in \mathbb{Z}_p^n$. 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 $(S+T)\bigcap V$ is nonempty if and only if $\sum_{\mathbf{x}\in V} \alpha(\mathbf{x}) > 0$.

1.1.3. Basic properties of finite Fourier series.

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. Meanwhile by viewing $\mathbb{Z}_p^n$ as a $\mathbb{Z}$-module, the Gauss sum

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

is well defined whether we take $\mathbf{y} \in \mathbb{Z}^n$ or $\mathbf{y} \in \mathbb{Z}_p^n$. Let $\alpha(\mathbf{x})$, $\beta(\mathbf{x})$ be complex valued function 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

$$\alpha * \beta(\mathbf{x}) = \sum_{\mathbf{y}} p^n a(\mathbf{y})\,b(\mathbf{y})\,e_p(\mathbf{x}\cdot\mathbf{y}). \tag{1.6}$$

$$\alpha\beta(\mathbf{x}) = \alpha(\mathbf{x})\beta(\mathbf{x}) = \sum_{\mathbf{y}} (a*b)(\mathbf{y})\,e_p(\mathbf{x}\cdot\mathbf{y}). \tag{1.7}$$

$$\sum_{\mathbf{x}}(\alpha * \beta)(\mathbf{x}) = \Big(\sum_{\mathbf{x}}\alpha(\mathbf{x})\Big)\Big(\sum_{\mathbf{x}}\beta(\mathbf{x})\Big). \tag{1.8}$$

$$\sum_{\mathbf{x}}\big|(\alpha * \beta)(\mathbf{x})\big| \le \Big(\sum_{\mathbf{x}}\big|\alpha(\mathbf{x})\big|\Big)\Big(\sum_{\mathbf{x}}\big|\beta(\mathbf{x})\big|\Big). \tag{1.9}$$

$$\sum_{\mathbf{y}}\big|a(\mathbf{y})\big|^2 = p^{-n}\sum_{\mathbf{x}}\big|\alpha(\mathbf{x})\big|^2. \tag{1.10}$$

The last identity is Parseval's equality**.**

§1.2. A summary of Cochrane's technique.

In this section we give a summary of the strategy that Cochrane follows to find a small solution of a quadratic form modulo p (for more details see [**5**], [**6**], [**8**]).

Let $Q(\mathbf{x}) = Q(x_1,...,x_n)$ be a quadratic form with integer coefficients and p be an odd prime. Set $\|\mathbf{x}\| = \max|x_i|$. Let $V = V_p(Q)$ be the set of zeros of Q contained in $\mathbb{Z}_p^n$. When n is even we let

$$\Delta_p(Q) = \begin{cases} \Big((-1)^{n/2}\det Q\,/\,p\Big) & \text{if} \quad p\nmid \det Q, \\ 0 & \text{if} \quad p\,\Big|\,\det Q, \end{cases}$$

where $(\cdot/p)$ is the Legendre symbol.

We outline the key ideas of Cochrane's technique for obtaining small solutions of

$$Q(\mathbf{x}) \equiv 0 \pmod p, \tag{1.11}$$

in the case when n is even.

1.2.1. Determination of $\phi(V,\mathbf{y})$ modulo p.

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

Lemma 1.1. [see e.g.[**5**], Lemma 1] *When n even and $\Delta = \pm 1$,*

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

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

1.2.2. Fundamental identity.

Recall, in (1.4) we saw the identity

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

Inserting the value $\phi(V,\mathbf{y})$ in Lemma 1.1 yields (see e.g. [**5**]),

Lemma 1.2. [**The fundamental identity**] Suppose n is even. *For any* $\alpha(\mathbf{x})$ *on* $\mathbb{Z}_p^n$, *and any quadratic form* $Q(\mathbf{x})$ *with* $\Delta_p(Q) = \pm 1$,

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

1.2.3. Small solutions of the quadratic congruence

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

Let our set $\mathscr{B}$ be a box of points of the type

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

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

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

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

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

$$\begin{aligned}\sum_{\mathbf{x}\in\mathbf{V}}\alpha(\mathbf{x}) &> \frac{1}{p}\sum_{\mathbf{x}}\alpha(\mathbf{x}) - \alpha(\mathbf{0})p^{(n/2)-1}\\ &= \frac{|\mathscr{B}_1|^2}{p} - |\mathscr{B}_1|\,p^{(n/2)-1}.\end{aligned}$$

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

2) $\Delta=-1$. In this case we need to estimate $\sum_{Q^*(\mathbf{y})=\mathbf{0}}a(\mathbf{y})$, but we don't insist on $\mathscr{B}$ 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 $|V\bigcap\mathscr{B}|$, the number of solutions of (1.11) with $\mathbf{x}\in\mathscr{B}$. First [**8**] establishes,

Lemma 1.3. [[**8**], Lemma 1] *Let S be a closed star-shaped region about the origin in $\mathbb{R}^n$ with $\|x\|<p/2$ 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*

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

Then using the fundamental identity and lemma 1.3 one obtains

Lemma 1.4. [[**8**], Lemma 2] *Suppose that $n\geq 4$ is even, $\Delta_p(Q)=-1$ and $V=V_p(Q)$. Let $\mathscr{B}$ be a box of points of the type*

$$\mathscr{B}=\left\{\mathbf{y}\in\mathbb{Z}_p^n\,\middle|\,|y_i|\leq B_i,1\leq i\leq n\right\},$$

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

$$|\mathscr{B}\bigcap V|\leq 2^{n^2+(3+t)n+1}\frac{|\mathscr{B}|}{p}+\frac{1}{2^t}p^{n/2-1}.$$

A second appeal to the fundamental identity yields

Theorem 1.1. [[**8**], Theorem 2] *Suppose that $n\geq 4$ is even, $p\geq 2^{4n+6}10^{2n-2}$ and that $\Delta_p(Q)=-1$. If*

$$m_i\geq 2^{5n+7}10^n \quad \textit{for} \quad 1\leq i\leq n, \quad \textit{and} \quad |\mathscr{B}|>2^{3n^2+4n+2}10^n p^{n/2},$$

then $\mathscr{B}$ *contains a nonzero solution of* (1.11).

The next theorem follows from Theorem 1.1 upon setting all but 4 variables equal to zero and letting $\mathscr{B}$ be a cube centered about the origin.

Theorem 1.2. [[**8**], Theorem 1] *For any quadratic form* $Q(\mathbf{x})$ *with* $n \geq 4$ *and any prime* p, *there exists a nonzero solution* $\mathbf{x}$ *of* (1.12) *with*

$$\|\mathbf{x}\| < \max\left\{2^{19}p^{1/2}, 2^{22}10^6\right\}, \tag{1.12}$$

§ 1.3. A small improvement of Cochrane's estimate.

By a little work, the bound (1.12) in last section can be improved to the following.

Theorem 1.3. *For any quadratic form* $Q(\mathbf{x})$ *with* $n \geq 4$ *and any prime* p, *there exists a nonzero solution* $\mathbf{x}$ *of* (1.11) *with*

$$\|\mathbf{x}\| < \min\left\{p^{2/3}, 2^{19}p^{1/2}\right\}. \tag{1.13}$$

Proof. By setting variables equal to zero, we may assume $n = 4$. The bound in [**17**] gives for $n \geq 2$, a nonzero solution $\mathbf{x}$ of (1.11) with

$$\|\mathbf{x}\| \leq \begin{cases} p^{1/2+1/2n} & \text{if } n \text{ odd}, \\ p^{1/2+1/2(n-1)} & \text{if } n \text{ even}. \end{cases} \tag{1.14}$$

When $n = 4$ (1.14) gives

$$\|\mathbf{x}\| \leq p^{2/3}. \tag{1.15}$$

We combine this upper bound with the bound of Theorem 1.2. The two upper bounds are graphed in figure 1.1 below. Observe that

$$\begin{aligned} 2^{19}p^{1/2} = 2^{22}10^6 &\iff p^{1/2} = 2^3 10^6 \\ &\iff p = 2^6 10^{12} = 6.4 \times 10^{13}. \end{aligned} \tag{1.16}$$

On the other hand, comparing (1.15) and (1.12), we have that

$$\begin{aligned} p^{2/3} = 2^{19}p^{1/2} &\iff p^{1/6} = 2^{19} \\ &\iff p = 2^{19\cdot 6} = 2 \times 10^{34}, \end{aligned} \tag{1.17}$$

and

$$p^{2/3} = 2^{22}10^6 \iff p = 2^{22\cdot 3/2}10^{6\cdot 3/2} = 2^{33}10^9 = 8.59 \times 10^{18}. \tag{1.18}$$

So collecting (1.16), (1.17), (1.18), one deduces that if $p < 2^{114}$, we use $\|\mathbf{x}\| < p^{2/3}$ and if $p > 2^{114}$ we use $\|\mathbf{x}\| < 2^{19} p^{1/2}$ (see figure 1.1). Thus (1.13) follows. □

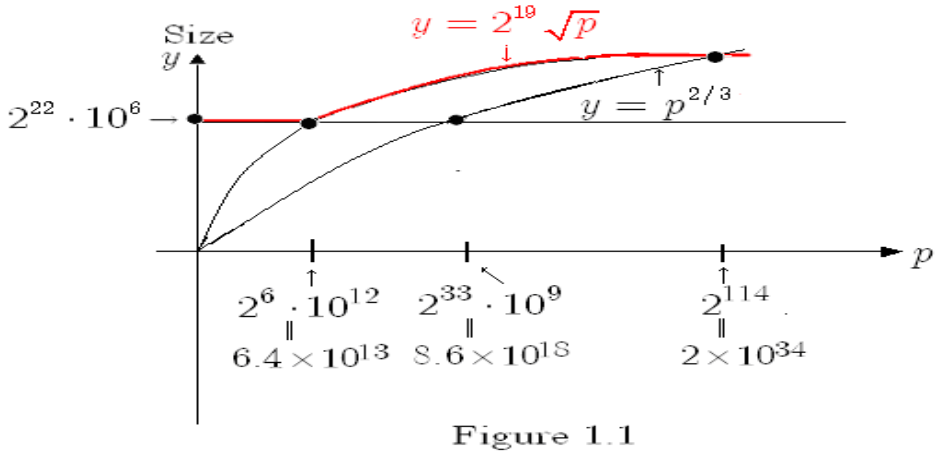

Figure 1.1

§1.4. Exponential sums modulo p^m.

In order to proceed from congruences (mod p) to congruences (mod p^m), we need to generalize results for exponential sums. Let $\mathbb{Z}_{p^m} = \mathbb{Z}/(p^m)$. Again we have the basic orthogonality relationship that for any $\mathbf{y} \in \mathbb{Z}_{p^m}^n$,

$$\sum_{\mathbf{x} \in \mathbb{Z}_{p^m}^n} e_{p^m}(\mathbf{x} \cdot \mathbf{y}) = \begin{cases} p^{mn} & \text{if} \quad \mathbf{y} = \mathbf{0}, \\ 0 & \text{if} \quad \mathbf{y} \neq \mathbf{0}. \end{cases} \tag{1.19}$$

We also will use the following lemma many times. Let $G(p^m)$ denote the multiplicative group of units modulo p^m.

Lemma 1.5. *Let $\lambda, a \in \mathbb{Z}$. For any odd prime p and any positive integer m,*

$$\sum_{\lambda \in G(p^m)} e_{p^m}(\lambda a) = \begin{cases} p^m - p^{m-1} & \text{if} \quad p^m \mid a, \\ -p^{m-1} & \text{if} \quad p^{m-1} \| a, \\ 0 & \text{if} \quad p^{m-1} \nmid a. \end{cases}$$

Proof. The sum $\sum_{\lambda \in G(p^m)} e_p(\lambda a)$ my be written as follows:

$$\sum_{\lambda\in G(p^m)} e_{p^m}(\lambda a) = \sum_{\lambda=1}^{p^m} e_{p^m}(\lambda a) - \sum_{p|\lambda} e_{p^m}(\lambda a).$$

Now, it is well known that

$$\sum_{\lambda=1}^{p^m} e_{p^m}(\lambda a) = \begin{cases} 0 & \text{if} \quad p^m \nmid a, \\ p^m & \text{if} \quad p^m \,|a. \end{cases} \tag{1.20}$$

So for the second sum if we set $\lambda = p\lambda'$, we have (using (1.20))

$$\sum_{p|\lambda} e_{p^m}(\lambda a) = \sum_{\lambda'=1}^{p^{m-1}} e_{p^m}(p\lambda' a) = \sum_{\lambda'=1}^{p^{m-1}} e_{p^{m-1}}(\lambda' a) \overset{(1.20)}{=} \begin{cases} 0 & \text{if} \quad p^{m-1} \nmid a, \\ p^{m-1} & \text{if} \quad p^{m-1} \,|a. \end{cases}$$

Therefore,

$$\sum_{\lambda\in G(p^m)} e_{p^m}(\lambda a) = \begin{cases} 0 & \text{if} \quad p^{m-1} \nmid a \\ 0 - p^{m-1} & \text{if} \quad p^{m-1} \| a \\ p^m - p^{m\text{-}1} & \text{if} \quad p^m \,|a. \end{cases}$$

This completes the proof of Lemma 1.5.□

Let f be a polynomial with integer coefficients and let

$$S(f, p^m) = \sum_{x=1}^{p^m} e_{p^m}\big(f(x)\big),$$

where p^m is a prime power with $m \geq 2$. For any polynomial f over $\mathbb{Z}$ we define

$$t = t(f) \coloneqq \operatorname{ord}_p\big(f'(X)\big),$$

where $f' = f'(X)$ denotes the derivative of $f(X)$. Also we define the set of critical points associated with the sum $S(f, p^m)$ to be the set

$$\mathcal{A} = \mathcal{A}(f, p) \coloneqq \{\alpha_1, ..., \alpha_D\},$$

of zeros of the congruence

$$p^{-t} f'(x) \equiv 0 \pmod p, \tag{1.21}$$

where $t = \operatorname{ord}_p(f')$. For any $\alpha \in \mathcal{A}$ let $\nu = \nu_\alpha$ denote the multiplicity of α as a zero of the congruence (1.21).

Theorem 1.4. [[**11**], Theorem 2.1]: *Let p be an odd prime and f be a non-constant polynomial defined over $\mathbb{Z}$. If $m \geq t+2$ then for any integer α we have:*

(i) *If* $\alpha \notin \mathcal{A}$ *then* $S_\alpha(f,p^m)=0$.

(ii) *If* α *is a critical point of multiplicity* ν *then*

$$\left|S_\alpha(f,p^m)\right| \le \nu p^{t/(\nu+1)} p^{(m(1-1/(\nu+1))}. \tag{1.22}$$

(iii) *If* α *is a critical point of multiplicity one then*

$$S_\alpha(f,p^m)=\begin{cases} e_{p^m}\left(f(\alpha^*)\right)p^{(m+t)/2} & \text{if } m-t \text{ is even},\\ \chi_2\left(A_\alpha\right)e_{p^m}\left(f(\alpha^*)\right)G_p p^{(m+t-1)/2} & \text{if } m-t \text{ is odd},\end{cases}$$

where α^* *is the unique lifting of* α^* *to a solution of the congruence* $p^{-t}f'(x)\equiv 0 \pmod{p^{[(m-t+1)/2]}}$, *and* $A_\alpha \equiv 2p^{-t}f''(\alpha^*)\pmod p$. *In particular, we have equality in* (1.22). *Here* G_p *is the classical Gauss sum,*

$$G_p := \sum_{x=1}^{p} e_p(x^2) = \begin{cases}\sqrt{p} & \text{if } p\equiv 1 \pmod 4,\\ i\sqrt{p} & \text{if } p\equiv 3 \pmod 4,\end{cases}$$

and χ_2 *is the quadratic character mod* p.

The proof of Theorem 1.4 is given in [**11**].

§1.5. Basic results on quadratic forms modulo p^m.

In this section we shall discuss as background for our work some of the general properties of quadratic forms over the ring $\mathbb{Z}_{p^m}=\mathbb{Z}/(p^m)$, with p an odd prime and m a positive integer.

1.5.1. Notations and Definitions.

Recall that a quadratic form $Q(\mathbf{x})$ over $\mathbb{Z}$ is a polynomial of the type

$$Q(\mathbf{x})=Q(x_1,x_2,\ldots,x_n)=\sum_{1\le i\le j\le n} a_{ij}x_i x_j\,,$$

with $a_{ij}\in\mathbb{Z}$, $1\le i\le j\le n$. We associate with $Q(\mathbf{x})$ a symmetric $n\times n$ matrix $A=A_Q$ given by

$$A_Q=\begin{bmatrix} a_{11} & \frac12 a_{12} & \frac12 a_{13} & \cdots & \frac12 a_{1n}\\ \frac12 a_{21} & a_{22} & \frac12 a_{23} & \cdots & \frac12 a_{2n}\\ \frac12 a_{31} & \frac12 a_{32} & a_{33} & \cdots & \frac12 a_{3n}\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ \frac12 a_{n1} & \frac12 a_{n2} & \frac12 a_{n3} & \cdots & a_{nn}\end{bmatrix}.$$

That is

$$A = [a^*_{ij}]_{n\times n}, \qquad a^*_{ij} = \begin{cases} \frac{1}{2}a_{ij} & \text{for } i < j, \\ \frac{1}{2}a_{ji} & \text{for } i > j, \\ a_{ii} & \text{for } i = j. \end{cases}$$

Observe that

$$Q(\mathbf{x}) = \mathbf{x}^t A \mathbf{x}$$

where

$$\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}, \qquad \mathbf{x}^t = [x_1 \quad x_2 \quad \dots \quad x_n].$$

Here $\mathbf{x}^t$ denotes the transpose of the matrix $\mathbf{x}$. On the other hand note that if the matrix A is diagonal (An $n\times n$ matrix A is diagonal if $a_{ij} = 0$ whenever $i \neq j$), then the corresponding quadratic form Q has the diagonal representation

$$Q(\mathbf{x}) = \mathbf{x}^t A \mathbf{x} = a_{11}x_1^2 + \cdots + a_{nn}x_n^2 ,$$

i.e., the quadratic form will contain no "cross product" terms. In the same way we call Q a diagonal quadratic form (mod p^m) for any prime power p^m if Q contain no "cross product" terms when read (mod p^m). The determinant of Q, abbreviated $\det Q$, is defined to be the determinant of the matrix A_Q. We say that $Q(\mathbf{x})$ is nonsingular over $\mathbb{Z}$ if $\det Q \neq 0$. Similarly for any odd prime power p^m we say $Q(\mathbf{x})$ is nonsingular mod p^m if $p \nmid \det Q$.

Again let p^m be an odd prime power. Let $Q(\mathbf{x})$ and $\tilde{Q}(\mathbf{x})$ be two quadratic forms over $\mathbb{Z}$ with associated matrices $A_Q, A_{\tilde{Q}}$ respectively. We now view the entries of these matrices as elements of $\mathbb{Z}/(p^m)$, and regard $1/2$ as the multiplicative inverse of $2 \pmod{p^m}$. (Alternatively we can replace ½ with $^{(p^m+1)}\!/_2$ and regard A_Q as having integer entries). We say that $Q(\mathbf{x})$ is equivalent to $\tilde{Q}(\mathbf{x}) \pmod{p^m}$, written $Q(\mathbf{x}) \sim \tilde{Q}(\mathbf{x}) \pmod{p^m}$, if there is an invertible $n\times n$ matrix T over $\mathbb{Z}/(p^m)$, such that $\tilde{Q}(\mathbf{x}) \equiv Q(T\mathbf{x}) \pmod{p^m}$, that is

$$A_{\tilde{Q}} \equiv T^t A_Q T \pmod{p^m}.$$

It is clear that " $\sim$ " is an equivalence relation. Note that

$$\det \tilde{Q} = \det Q \cdot (\det T)^2 \pmod{p^m}.$$

***Example*:** Let p^m be any odd prime power and $Q(\mathbf{x}) = x_1^2 + x_1x_2 + x_2^2$. Then

$$Q(\mathbf{x}) = \mathbf{x}^t A \mathbf{x},$$

where

$$A = \begin{bmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{bmatrix}.$$

That is

$$Q(\mathbf{x}) = x_1^2 + x_1x_2 + x_2^2 = \underbrace{\begin{bmatrix} x_1 & x_2 \end{bmatrix}}_{\mathbf{x}^t} \underbrace{\begin{bmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{bmatrix}}_{A_Q} \underbrace{\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}}_{\mathbf{x}}.$$

By making the simple observation that

$$Q(\mathbf{x}) = x_1^2 + x_1x_2 + x_2^2 \equiv x_1^2 + \underbrace{(p^m + 1)}_{\text{even}} x_1x_2 + x_2^2 \pmod{p^m},$$

we can write

$$Q(\mathbf{x}) \equiv \mathbf{x}^t A' \mathbf{x} \pmod{p^m},$$

with

$$A' = \begin{bmatrix} 1 & \frac{p^m+1}{2} \\ \frac{p^m+1}{2} & 1 \end{bmatrix} \in M_{2\times 2}(\mathbb{Z}).$$

Note that since p is odd, the entries of A' are all integers. Thus we may assume that $A_Q \in M_{2\times 2}(\mathbb{Z})$ when working with congruences modulo odd primes.

1.5.2. Diagonalization of quadratic forms modulo p^m.

In this subsection we prove

Theorem 1.5. *For any odd prime power p^m, and quadratic form $Q(\mathbf{x})$ over $\mathbb{Z}$, $Q(\mathbf{x})$ is equivalent to a diagonal quadratic form (modulo p^m).*

1.5.2. Diagonalization of quadratic forms modulo p^m.

In this subsection we prove

Theorem 1.5. *For any odd prime power p^m, and quadratic form $Q(\mathbf{x})$ over $\mathbb{Z}$, $Q(\mathbf{x})$ is equivalent to a diagonal quadratic form (modulo p^m).*

Proof. The theorem is well known and a proof can be found for example in [**25**]. We shall only deal with the case of nonsingular $Q \pmod p$, the type of form we deal with in this thesis. We proceed by induction on m. When $m = 1$, it is well known (see [**29**]) that Q can be diagonalized over the finite field $\mathbb{F}_p$. Say

$$T^t A_Q T \equiv D \pmod p,$$

for some $T, D \in M_{n\times n}(\mathbb{Z})$ with T nonsingular $\pmod p$ and D a diagonal matrix. Lets lift this to a solution $\pmod{p^2}$. Let

$$U = T + pX ,$$

where $X = [x_{ij}]$ is a matrix of variables. We wish to solve

$$U^t A_Q U \equiv D \pmod{p^2}.$$

This is equivalent to

$$\begin{aligned} & (T + pX)^t A_Q (T + pX) \equiv D \pmod{p^2} \\ \iff\quad & T^t A\, T + T^t A_Q pX + pX^t A_Q T \equiv D \pmod{p^2} \\ \iff\quad & \frac{T^t A_Q T - D}{p} + \underbrace{T^t A_Q X}_{Y} + X^t A_Q T \equiv 0 \pmod p \\ \iff\quad & Y + Y^t \equiv \underbrace{\frac{D - T^t A_Q T}{p}}_{B} \pmod p, \end{aligned}$$

where $Y = T^t A_Q X$ and $B = (D - T^t A_Q T)/p$. Note that B is a symmetric matrix with integer entries. Let

$$Y \equiv \begin{bmatrix} \frac{1}{2}b_{11} & & & & \\ b_{21} & \frac{1}{2}b_{22} & & & \text{\huge 0} \\ b_{31} & b_{32} & \frac{1}{2}b_{33} & & \\ \vdots & \vdots & \vdots & \ddots & \\ b_{n1} & b_{n2} & b_{n3} & \cdots & \frac{1}{2}b_{nn} \end{bmatrix} \pmod{p^2}.$$

Then $Y + Y^t = B$. Thus we are left with solving the congruence

$$T^t A_Q X \equiv Y \pmod{p}.$$

Since T and A_Q are nonsingular $(\mathrm{mod}\, p)$, this equation has a unique solution $X \equiv A_Q^{-1}(T^t)^{-1}Y(\mathrm{mod}\, p)$.

In the same manner one can lift a solution $(\mathrm{mod}\, p^m)$, to $(\mathrm{mod}\, p^{m+1})$ for any m. Indeed, proceeding as above, suppose that

$$T^t A\, T \equiv D \pmod{p^m},$$

for some $T, D \in M_{n\times n}(\mathbb{Z})$ with T nonsingular $(\mathrm{mod}\, p)$ and D a diagonal matrix. Let

$$U = T + p^m X,$$

where X is a matrix of variables and solve

$$U^t A_Q U \equiv D \pmod{p^m}.$$

This is equivalent to

$$\begin{aligned}
& (T + p^m X)^t\, A(T + p^m X) \equiv D \,(\mathrm{mod}\, p^m) \\
\iff \quad & T^t A\, T + T^t A p^m X + p^m X^t A\, T \equiv D \,(\mathrm{mod}\, p^{m+1}) \\
\iff \quad & \frac{T^t A\, T - D}{p^m} + \underbrace{T^t A X}_{Y} + X^t A\, T \equiv 0 \,(\mathrm{mod}\, p) \\
\iff \quad & Y + Y^t \equiv \underbrace{\frac{D - T^t A\, T}{p^m}}_{B} \,(\mathrm{mod}\, p),
\end{aligned}$$

where $Y = T^t A X$ and $B = (D - T^t A\, T)/\, p^m$ is a symmetric matrix with integer entries. Let

$$Y \equiv \begin{bmatrix}
\frac{1}{2}\beta_{11} & & & & \\
\beta_{21} & \frac{1}{2}\beta_{22} & & & \\
\beta_{31} & \beta_{32} & \frac{1}{2}\beta_{33} & & \\
\vdots & \vdots & \vdots & \ddots & \\
\beta_{n1} & \beta_{n2} & \beta_{n3} & \cdots & \frac{1}{2}\beta_{nn}
\end{bmatrix} \mathbf{0} \pmod{p^m}.$$

Then $Y + Y^t = B$ (We note that the choice of Y is not unique). Hence we are left with solving the congruence

$$T^t A X \equiv Y \pmod{p}.$$

As T and A are nonsingular $(\mathrm{mod}\, p)$, this equation has a unique solution

$X \equiv A^{-1}(T^t)^{-1}Y(\mathrm{mod}\, p^m)$. This completes the induction step. □

***Examples*: 1.** Let

$$Q(x,y) = [x \;\; y]\overbrace{\begin{bmatrix} 1 & \frac{p}{2} \\ \frac{p}{2} & 1 \end{bmatrix}}^{A}\begin{bmatrix} x \\ y \end{bmatrix} = x^2 + pxy + y^2.$$

Note that $Q(x,y)$ is already a diagonal form when read $(\mathrm{mod}\, p)$. We proceed to diagonalize $Q(x,y)$ $(\mathrm{mod}\, p^2)$.

$$T = I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

$$B = \frac{D - T^t A\, T}{p} = \frac{1}{p}\left[\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} - \begin{bmatrix} 1 & \frac{p}{2} \\ \frac{p}{2} & 1 \end{bmatrix}\right] = \begin{bmatrix} 0 & \frac{-1}{2} \\ \frac{-1}{2} & 0 \end{bmatrix} = -\frac{1}{2}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

$$Y = \begin{bmatrix} 0 & 0 \\ \frac{-1}{2} & 0 \end{bmatrix}.$$

Solve $AX \equiv Y(\mathrm{mod}\, p)$,

$$\begin{bmatrix} 1 & \frac{p}{2} \\ \frac{p}{2} & 1 \end{bmatrix}\begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix} \equiv \begin{bmatrix} 0 & 0 \\ \frac{-1}{2} & 0 \end{bmatrix} \quad (\mathrm{mod}\, p)$$

$$\iff \quad \frac{1}{2}\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}\begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix} \equiv -\frac{1}{2}\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \quad (\mathrm{mod}\, p)$$

$$\iff \quad \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix} \equiv \begin{bmatrix} 0 & 0 \\ \frac{-1}{2} & 0 \end{bmatrix} \quad (\mathrm{mod}\, p).$$

***Check* :**

$$U = T + pX = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + p\begin{bmatrix} 0 & 0 \\ \frac{-1}{2} & 0 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ \frac{-p}{2} & 1 \end{bmatrix}$$

$$U^t A\, U = \begin{bmatrix} 1 & \frac{-p}{2} \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & \frac{p}{2} \\ \frac{p}{2} & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ \frac{-p}{2} & 1 \end{bmatrix} \equiv \begin{bmatrix} 1 & \frac{-p}{2} \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & \frac{p}{2} \\ 0 & 1 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad (\mathrm{mod}\, p^2).$$

Thus $Q(\mathbf{x}) \sim x^2 + y^2$ $(\mathrm{mod}\, p^2)$.

2. Let

$$Q(x,y) = [x \;\; y]\overbrace{\begin{bmatrix} 1 & \frac{p}{2} \\ \frac{p}{2} & 0 \end{bmatrix}}^{A}\begin{bmatrix} x \\ y \end{bmatrix} = x^2 + pxy \equiv x^2(\mathrm{mod}\, p).$$

What happens if A singular?

Here A is not invertible, so we cannot directly follow the method given in our proof. Let us try to solve

$$T^tAX \equiv Y \pmod{p}.$$

First, we see that $T = I_2$ since A is already diagonal $(\bmod p)$. Let $\frac{1}{2} \mapsto \frac{(p^2+1)}{2}$. Then

$$A = \begin{bmatrix} 1 & \frac{p}{2} \\ \frac{p}{2} & 0 \end{bmatrix} \equiv \begin{bmatrix} 1 & p\frac{p^2+1}{2} \\ p\frac{p^2+1}{2} & 0 \end{bmatrix} \pmod{p^2},$$

and the latter matrix has integer entries.

$$B = \frac{D-A}{p} = \frac{1}{p}\left[\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} 1 & p\frac{p^2+1}{2} \\ p\frac{p^2+1}{2} & 0 \end{bmatrix}\right] = \begin{bmatrix} 0 & -\frac{p^2+1}{2} \\ -\frac{p^2+1}{2} & 0 \end{bmatrix}.$$

If we proceed as in the proof we would let

$$Y = \begin{bmatrix} 0 & 0 \\ -\frac{p^2+1}{2} & 0 \end{bmatrix} \pmod{p^2}.$$

Now solve

$$\begin{bmatrix} 1 & p\frac{p^2+1}{2} \\ p\frac{p^2+1}{2} & 0 \end{bmatrix} X \equiv \begin{bmatrix} 0 & 0 \\ -\frac{p^2+1}{2} & 0 \end{bmatrix} \pmod{p}.$$

This is equivalent to

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix} \equiv \begin{bmatrix} 0 & 0 \\ \frac{-1}{2} & 0 \end{bmatrix} \pmod{p}$$

$$\iff \quad \begin{bmatrix} x_{11} & x_{12} \\ 0 & 0 \end{bmatrix} \equiv \begin{bmatrix} 0 & 0 \\ \frac{-1}{2} & 0 \end{bmatrix} \pmod{p},$$

which give us a contradiction $(0 = {}^{-1}\!/_{2})$ and hence there is no solution of this system.

Next, let us try the choice

$$Y = \begin{bmatrix} 0 & \alpha \\ -\frac{p^2+1}{2} - \alpha & 0 \end{bmatrix} \pmod{p^2}.$$

Then

$$Y + Y^t = \begin{bmatrix} 0 & \alpha \\ -\frac{p^2+1}{2} - \alpha & 0 \end{bmatrix} + \begin{bmatrix} 0 & -\frac{p^2+1}{2} - \alpha \\ \alpha & 0 \end{bmatrix} = B \pmod{p^2}.$$

Solve

$$\begin{bmatrix} 1 & p\frac{p^2+1}{2} \\ p\frac{p^2+1}{2} & 0 \end{bmatrix} X \equiv \begin{bmatrix} 0 & \alpha \\ -\frac{p^2+1}{2} - \alpha & 0 \end{bmatrix} \pmod{p},$$

or, equivalently

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix} \equiv \begin{bmatrix} 0 & 0+\alpha \\ \frac{-1}{2} - \alpha & 0 \end{bmatrix} \pmod{p}.$$

Let $\alpha = -\frac{1}{2}$. Then obviously

$$\begin{bmatrix} x_{11} & x_{12} \\ 0 & 0 \end{bmatrix} \equiv \begin{bmatrix} 0 & \frac{-1}{2} \\ 0 & 0 \end{bmatrix} \pmod{p},$$

so that

$$X = \begin{bmatrix} 0 & \frac{-1}{2} \\ 0 & 0 \end{bmatrix}.$$

Hence, it follows one can make the change of variable

$$x \mapsto x + p\frac{p-1}{2}y, \quad y \mapsto y$$

to diagonlize the quadratic form $Q(x,y) \pmod{p^2}$. Indeed,

$$\begin{aligned} x^2 + pxy &\sim \left(x + \tfrac{p-1}{2}py\right)^2 + p\left(x + p\tfrac{p-1}{2}py\right)y \\ &\equiv (p-1)pxy + x^2 + pxy \pmod{p^2} \\ &\equiv x^2 \pmod{p^2}. \end{aligned}$$

Our proof of Theorem 1.5 actually yields the stronger result.

Corollary 1.1. *If p is an odd prime, $Q(\mathbf{x})$ is a quadratic form over $\mathbb{Z}$, nonsingular $\pmod{p}$ and equivalent to diagonal form $\sum_{i=1}^n a_i x_i^2 \pmod{p}$, then $Q(\mathbf{x})$ is equivalent to the same diagonal form $\sum_{i=1}^n a_i x_i^2 \pmod{p^m}$ for any m.*

***Note*:** This fails for nonsingular forms. Indeed $x^2 + py^2 \sim x^2 \pmod{p}$, but $x^2 + py^2 \not\sim x^2 \pmod{p^2}$.

Chapter 2

Small Zeros of Quadratic Forms Modulo p^2

§2.1 Introduction.

Let $Q(\mathbf{x}) = Q(x_1, x_2, ..., x_n) = \sum_{1 \le i \le j \le n} a_{ij} x_i x_j$ be a quadratic form with integer coefficients and p be an odd prime. Set $\|\mathbf{x}\| = \max |x_i|$. Let $V_{p^2} = V_{p^2}(Q)$ be the set of zeros of Q contained in $\mathbb{Z}_{p^2}^n$. When n is even we let

$$\Delta_p(Q) = \begin{cases} \left((-1)^{n/2} \det A_Q \,/\, p \right) & \text{if} \quad p \nmid \det A_Q, \\ 0 & \text{if} \quad p \mid \det A_Q, \end{cases}$$

where $(\bullet / p)$ denotes the Legendre-Jacobi symbol and A_Q is the $n \times n$ defining matrix for $Q(\mathrm{x})$. For $\mathbf{y} \in \mathbb{Z}_{p^2}^n$ set

$$\phi(V, \mathbf{y}) = \begin{cases} \sum_{\mathbf{x} \in V} e_{p^2}(\mathbf{x} \cdot \mathbf{y}) & \text{for} \quad \mathbf{y} \not\equiv \mathbf{0}, \\ |V| - p^{2(n-1)} & \text{for} \quad \mathbf{y} = \mathbf{0}, \end{cases}$$

where $e_{p^2}(x) = e^{2\pi i x / p^2}$. Our goal in this chapter is to generalize $(\bmod p)$ methods for obtaining a small primitive solution of

$$Q(\mathbf{x}) \equiv 0 \pmod{p^2}. \tag{2.1}$$

Recall by primitive we mean $p \nmid x_i$ for some i. By small we mean $\|\mathbf{x}\| \le C(p^2)^{\delta}$, for some $\delta > 0$ and constant C. Ideally, we would like $\|\mathbf{x}\| < p$. Note, one has trivial nonzero small solutions of (2.1) such as

$(p,0,0,\ldots,0)$, but these solutions are not primitive. Our strategy is to first calculate the Gauss sum

$$S = S(f,p^2) = \sum_{x=1}^{p^2} e_{p^2}\left(\lambda a x^2 + xy\right), \tag{2.2}$$

and then use this sum to calculate the function $\phi(V,\mathbf{y})$. After that we use this calculation to find a fundamental identity analogous to Lemma 1.3. Finally we proceed to bound the error terms in the fundamental identity.

We can state our main result in this chapter; see Corollary 2.2 and Corollary 2.5.

Theorem 2.1. *For any odd prime p and nonsingular quadratic form $Q(\mathbf{x})$ with $n \geq 4$, n even, there exists a primitive solution of (2.1) with*

$$\|\mathrm{x}\| \leq \begin{cases} \max\left\{2^5 p, 2^{18}\right\} & \text{for } \Delta = +1, \quad (2.3) \\ \max\left\{2^5 p, 2^9\right\} & \text{for } \Delta = -1. \quad (2.4) \end{cases}$$

§2.2. Determination of $\phi(V,\mathbf{y})$ modulo p^2.

2.2.1. Calculating the sum $S(f,p^2)$.

We need to use Theorem 1.4 of Chapter 1 with $m=2$. The following fundamental lemma holds.

Lemma 2.1. *Let p be an odd prime, $\lambda, a, y \in \mathbb{Z}$ with $p \nmid a$ and S be as in (2.2). Then*

$$S = \begin{cases} e_{p^2}(-\overline{4}\overline{a}\overline{\lambda}\, y^2)p & \text{if} \quad p \nmid \lambda, \\ p\,\chi(\lambda' a) G_p\, e_p\left(-\overline{4}\overline{\lambda}'\overline{a} y'^2\right) & \text{if } p \| \lambda \text{ and } p \mid y, \\ 0 & \text{if } p \| \lambda \text{ and } p \nmid y, \end{cases}$$

where χ is Legendre Symbol , $\lambda' = \lambda p^{-1}$, $y' = y p^{-1}$, and $\overline{\lambda}, \overline{\lambda}', \overline{a}$ are inverses $\bmod p^2$.

Proof. Assume that $p \nmid a$. We consider two cases:

***Case* (i):** $p \nmid \lambda$. The critical point congruence is

$$p^{-t} f'(x) \equiv 0 \pmod{p},$$

or, equivalently

$$p^{-t}(2\lambda a x + y) \equiv 0 \pmod{p}, \tag{2.5}$$

where $t = \operatorname{ord}_p(f')$. Then clearly

$$p^t \| (2a\lambda, y) \quad \Rightarrow \quad t = 0,$$

because $p \nmid 2a\lambda$. Thus by applying (Theorem 1.4, part (iii)) we have $m - t = 2 - 0 = 2$ (even). So turning back to (2.5), we now have

$$2\lambda a x \equiv -y \pmod{p},$$

and hence

$$\alpha = x \equiv -\overline{2a\lambda}\, y \pmod{p}.$$

Thus

$$S = S_\alpha = e_{p^2}\big(f(\alpha^*)\big)\, p^{(2+t)/2} = e_{p^2}\big(\lambda a \alpha^{*2} + y\alpha^*\big)\, p\,,$$

where α^* is the unique lifting of α to a solution of (2.5) $\bmod p^{[3/2]} = \bmod p$. We take $\alpha^* \equiv -\overline{2}\,\overline{a}\,\overline{\lambda}\, y \pmod{p^2}$ where $\overline{2}, \overline{a}, \overline{\lambda}$ are inverses $\bmod p^2$. Then

$$\begin{aligned} f(\alpha^*) = \lambda a \alpha^{*2} + y\alpha^* &\equiv \lambda a (\overline{2a\lambda})^2 y^2 + (-1) y \overline{2a\lambda}\, y \pmod{p^2} \\ &\equiv \lambda a \overline{2}^2 \overline{a}^2 \overline{\lambda}^2 y^2 - \overline{2}\,\overline{a}\,\overline{\lambda}\, y^2 \pmod{p^2} \\ &\equiv \overline{\lambda}\overline{a}\overline{4} y^2 - \overline{2}\,\overline{a}\,\overline{\lambda}\, y^2 \pmod{p^2} \\ &\equiv -\overline{4}\overline{a}\overline{\lambda}\, y^2 \pmod{p^2}, \end{aligned}$$

and so $S_\alpha = e_{p^2}(-\overline{4}\overline{a}\overline{\lambda}\, y^2) p$.

***Case* (ii):** $p \| \lambda$, then again the critical point congruence is as in (2.5). Now if

1) $$p \,|\, y \quad \Rightarrow \quad t = 1\,,$$

since $p^t \,\|\, (2a\lambda, y)$, $p \,|\, (\lambda, y)$, and $p \nmid 2a$. Thus by setting $\lambda' = \lambda p^{-1}$, and $y' = y p^{-1}$, we have

$$S = \sum_{x=1}^{p^2} e_{p^2}\big(\lambda a x^2 + xy\big) = \sum_{x=1}^{p^2} e_{p^2}\big(p\lambda' a x^2 + p x y'\big)$$

$$= p\sum_{x=1}^{p} e_p(\lambda' a x^2 + xy') = p\,\chi(\lambda' a) G_p\, e_p\Big(\frac{-y'^2}{4\lambda' a}\Big).$$

So $S = p\,\chi(\lambda' a) G_p\, e_p\big(-\overline{4}\overline{\lambda}'\overline{a} y'^2\big)$.

2) $$p \nmid y \quad \Rightarrow \quad t = 0\,,$$

because $p^t \parallel (2a\lambda, y)$, and $p \nmid (2a, y)$. Returning, once more, to (2.5), we now have

$$2\lambda a x \equiv -y \,(\mathrm{mod}\, p)\,,$$

or, equivalently

$$0 \equiv -y \,(\mathrm{mod}\, p)\,,$$

a contradiction. Thus there is no critical point, so $S = 0$. Lemma 2.1 is completely proved. □

2.2.2. Evaluating $\phi(V, \mathbf{y})$ for the case of a diagonal quadratic form.

Assume that $Q(\mathbf{x}) = \sum_{i=1}^{n} a_i x_i^2$, with $p \nmid a_i$, $1 \le i \le n$. Then it follows from the orthogonality property of exponential sums that

$$\begin{aligned}\sum_{\mathbf{x}\in\mathbf{V}} e_{p^2}(\mathbf{x}\cdot\mathbf{y}) &= \sum_{\mathbf{x}\in\mathbb{Z}_{p^2}^n} p^{-2}\Big(\sum_{\lambda=0}^{p^2-1} e_{p^2}\left(\lambda Q(\mathbf{x})\right)\Big) e_{p^2}(\mathbf{x}\cdot\mathbf{y}) \\ &= p^{-2}\sum_{\lambda}\sum_{\mathbf{x}} e_{p^2}(\lambda Q(\mathbf{x}) + \mathbf{x}\cdot\mathbf{y}) \\ &= \underbrace{p^{-2}\sum_{\mathbf{x}} e_{p^2}(\mathbf{x}\cdot\mathbf{y})}_{S_1} + \underbrace{p^{-2}\sum_{\lambda\neq 0}\sum_{\mathbf{x}} e_{p^2}(\lambda Q(\mathbf{x}) + \mathbf{x}\cdot\mathbf{y})}_{S_2}.\end{aligned}$$

Now, if $\mathbf{y} = \mathbf{0}$, then we have

$$|V| = p^{2(n-1)} + S_2 \quad \Rightarrow \quad S_2 = |V| - p^{2(n-1)} = \phi(V, \mathbf{0})\,.$$

If $\mathbf{y} \neq \mathbf{0}$. Then, by (1.19) of Chapter 1, since some $y_i \neq 0$,

$$S_1 = p^{-2}\sum_{\mathbf{x}} e_{p^2}(\mathbf{x}\cdot\mathbf{y}) = p^{-2}\prod_{i=1}^{n}\sum_{x_i=1}^{p^2} e_{p^2}(x_i y_i) = 0.$$

Also,

$$S_2 = p^{-2}\sum_{\lambda\neq 0}\sum_{\mathbf{x}} e_{p^2}(\lambda Q(\mathbf{x}) + \mathbf{x}\cdot\mathbf{y})$$

$$= p^{-2}\sum_{\lambda\neq 0}\underbrace{\sum_{\mathbf{x}} e_{p^2}\left(\lambda(a_1x_1^2+a_2x_2^2+\cdots+a_nx_n^2)+x_1y_1+x_2y_2+\cdots+x_ny_n\right)}_{S_\lambda}.$$

Thus we now have $S_2=\phi(V,\mathbf{y})$ for all $\mathbf{y}$. Henceforth we shall use $\phi(V,\mathbf{y})$ to mean S_2 and vice versa. But first we need to treat the inside sum S_λ separately.

2.2.3. The sum S_λ.

We rewrite S_λ as follows:

$$\begin{aligned} S_\lambda &= \sum_{\mathbf{x}} e_{p^2}\left([\lambda a_1x_1^2+x_1y_1]+\cdots+[\lambda a_nx_n^2+y_nx_n]\right)\\ &= \sum_{x_1} e_{p^2}(\lambda a_1x_1^2+y_1x_1)\cdots\sum_{x_n} e_{p^2}(\lambda a_nx_n^2+y_nx_n)\\ &= \prod_{i=1}^{n}\underbrace{\sum_{x_i=1}^{p^2} e_{p^2}(\lambda a_ix_i^2+x_iy_i)}_{\text{Gauss sum}}. \end{aligned} \tag{2.6}$$

By $p|\mathbf{y}$ we shall mean that $p|y_i$ for all i and vice versa. As a consequence of Lemma 2.1 we have the following Lemma.

Lemma 2.2. *Let n be even and let S_λ be as in* (2.6). *Assume $p\nmid a_1,a_2,\ldots,a_n$. Then if $p^2\nmid\lambda$,*

$$S_\lambda=\begin{cases} 0 & \text{if } p|\lambda, \text{ and } p\nmid y_i \text{ for some } i,\\ p^n e_{p^2}\left(\overline{-4\lambda}\,Q^*(\mathbf{y})\right) & \text{if } p\nmid\lambda,\\ p^{3n/2}\Delta e_p\left(\overline{-4\lambda'}\,Q^*(\mathbf{y}')\right) & \text{if } p|\lambda, \text{ and } p\,|y_i \text{ for all } i, \end{cases}$$

where $\Delta=\chi\left((-1)^{n/2}\right)\chi\left(a_1\cdots a_n\right)$ and $\chi=\chi_2$.

Proof. We will divide the proof into two cases according to whether p divides λ or not.

***Case* (i):** $p\nmid\lambda$. Then, by Lemma 2.1, for any $\mathbf{y}$,

$$\begin{aligned} S_\lambda &= e_{p^2}(\overline{-4a_1\lambda}\,y_1^2)p\cdot e_{p^2}(\overline{-4a_2\lambda}\,y_2^2)p\cdot\cdots\cdot e_{p^2}(\overline{-4a_n\lambda}\,y_n^2)p\\ &= p^n e_{p^2}(\underbrace{\overline{-4a_1\lambda}\,y_1^2+\overline{-4a_2\lambda}\,y_2^2+\cdots+\overline{-4a_n\lambda}\,y_n^2}_{-\overline{4}\,\overline{\lambda}Q^*(y_1,\ldots,y_n)=-\overline{4}\,\overline{\lambda}Q^*(\mathbf{y}),})\\ &= p^n e_{p^2}\left(-\overline{4}\,\overline{\lambda}Q^*(\mathbf{y})\right), \end{aligned}$$

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

***Case* (ii):** $p|\lambda$. Then we have the following two subcases:

1) $p \nmid y_i$ for some i. Then certainly, in view of Lemma 2.1, $S_\lambda = 0$.

2) $p|y_i$ for all i. Then again by Lemma 2.1,

$$\begin{aligned} S_\lambda &= p\,\chi(\lambda' a_1) G_p e_p(-\overline{4}\overline{a}_1\overline{\lambda}' y_1'^2) \cdots p\,\chi(\lambda a_n) G_p\, e_p(-\overline{4}\overline{a}_n\overline{\lambda}' y_n'^2) \\ &= p^n\, G_p^n\, \chi(\lambda' a_1 \cdots \lambda' a_n) e_p\Big(\overline{-4\lambda'}\; Q^*(y_1'^2 + y_2'^2 + \cdots + y_n'^2)\Big) \\ &= p^n p^{n/2} \overbrace{\chi\Big((-1)^{n/2}\Big)\, \underbrace{\chi(a_1 \cdots a_n)}_{n \text{ is even}}}^{\Delta}\, e_p\Big(\overline{-4\lambda'}\; Q^*(\mathbf{y}')\Big) \\ &= p^{3n/2} \Delta\, e_p\Big(\overline{-4\lambda'}\; Q^*(\mathbf{y}')\Big), \end{aligned}$$

and this completes the proof of Lemma 2.2. □

2.2.4. Formula for $\phi(V, \mathbf{y})$ for diagonal forms.

Lemma 2.3. *When n is even and $\Delta \neq 0$, Then*

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

where $\mathbf{y}' = \mathbf{y}p^{-1}$.

Proof. We have two cases:

***Case* (i):** $p \nmid y_i$ for some i. Then we first use Lemma 2.2, so obviously if $p|\lambda$, we have $S_\lambda = 0$ and

$$\begin{aligned} \phi(V,\mathbf{y}) &= p^{-2} \sum_{\substack{p|\lambda \\ \lambda \neq 0}} S_\lambda + \; p^{-2} \sum_{p \nmid \lambda} S_\lambda = p^{-2} \sum_{p \nmid \lambda} S_\lambda \\ &= p^{-2} p^n \sum_{p \nmid \lambda} e_{p^2}(-\overline{4}\overline{\lambda} Q^*(\mathbf{y})) \\ &= p^{n-2} \sum_{p \nmid \lambda} e_{p^2}\big(\lambda Q^*(\mathbf{y})\big), \end{aligned}$$

since $\overline{-4\lambda}$ runs through $G(p^m)$ as λ does. Next, we apply Lemma 1.5 of Chapter 1 to the last sum, to get

$$\phi(V,\mathbf{y}) = p^{n-2}\begin{cases} p^2-p & \text{if} \quad p^2 \,|\, Q^*(\mathbf{y}), \\ -p & \text{if} \quad p \,\|\, Q^*(\mathbf{y}), \\ 0 & \text{if} \quad p \nmid Q^*(\mathbf{y}). \end{cases} = \begin{cases} p^n - p^{n-1} & \text{if} \quad p^2 \,|\, Q^*(\mathbf{y}), \\ -p^{n-1} & \text{if} \quad p \,\|\, Q^*(\mathbf{y}), \\ 0 & \text{if} \quad p \nmid Q^*(\mathbf{y}). \end{cases}$$

***Case* (ii):** $p|y_i$ for all i, (that is, $p^2 \,|\, y_i^2 \ \ \forall i$ implies that $p^2 \,|\, Q^*(\mathbf{y})$). Then again by Lemma 2.2,

$$S_\lambda = \begin{cases} p^n & \text{if} \quad p \nmid \lambda, \\ p^{3n/2}\Delta e_p\left(-\overline{4}\overline{\lambda}' Q^*(\mathbf{y}')\right) & \text{if} \quad p|\lambda, \end{cases}$$

where $\lambda = p\lambda'$. Thus we now have

$$\begin{aligned} \phi(V,\mathbf{y}) &= p^{-2}\sum_{\substack{p|\lambda \\ \lambda \neq 0}} S_\lambda + p^{-2}\sum_{p\nmid\lambda} S_\lambda \\ &= p^{3n/2-2}\Delta\sum_{\lambda'=1}^{p-1} e_p\left(-\overline{4}\overline{\lambda}' Q^*(\mathbf{y}')\right) + p^{n-2}\sum_{p\nmid\lambda} 1. \\ &= p^{3n/2-2}\Delta \begin{cases} -1 & \text{if} \quad Q^*(\mathbf{y}') \not\equiv 0 \pmod p \\ p-1 & \text{if} \quad Q^*(\mathbf{y}') \equiv 0 \pmod p \end{cases} \quad + \quad p^{n-1}(p-1). \end{aligned}$$

It follows that

$$\phi(V,\mathbf{y}) = \begin{cases} -\Delta p^{3n/2-2} + p^{n-1}(p-1) & \text{if} \quad p \nmid Q^*(\mathbf{y}'), \\ \Delta(p-1)p^{3n/2-2} + p^{n-1}(p-1) & \text{if} \quad p \,|\, Q^*(\mathbf{y}'). \end{cases}$$

Combining cases (i) and (ii), Lemma 2.3 follows. □

2.2.5. Determination of $\phi(V,\mathbf{y})$ for a general quadratic form.

In the last section we calculated $\phi(V,\mathrm{y})$ for the case of diagonal quadratic forms. Suppose now that $Q(\mathrm{x})$ is any quadratic form. Let V_{p^2} be the set of solution of the quadratic congruence $Q(\mathbf{x}) \equiv 0 \pmod{p^2}$. Let $\mathbf{x} = T(\mathbf{u})$ where T is a transformation that diagonalizes Q, so that $Q(T(\mathbf{u})) = Q_1(\mathbf{u})$, a diagonal quadratic form. Let $V_{p^2}{}'$ be the set of solution of the quadratic congruence $Q_1(\mathbf{u}) \equiv 0 (\mathrm{mod}\, p^2)$. Set

$T^t(\mathbf{y}) = \mathbf{v}$. We first show that $\phi(V_{p^2}, \mathbf{y}) = \phi(V'_{p^2}, \mathbf{v})$. Note that, since T is a nonsingular transformation $\bmod p$, $\mathbf{y} \equiv \mathbf{0} (\bmod p)$ is equivalent to $\mathbf{v} \equiv \mathbf{0} (\bmod p)$. If $\mathbf{y} \equiv \mathbf{0} \pmod p$, then

$$\phi(V_{p^2}, \mathbf{y}) = \left|V_{p^2}\right| - p^{2(n-1)} = \left|V'_{p^2}\right| - p^{2(n-1)} = \phi(V'_{p^2}, \mathbf{v}).$$

For $\mathbf{y} \not\equiv \mathbf{0} \pmod p$, we have

$$\begin{aligned}
\phi(V_{p^2}, \mathbf{y}) &= \sum_{\mathbf{x} \in V_{p^2}} e_{p^2}(\mathbf{x} \cdot \mathbf{y}) \\
&= \sum_{Q(\mathbf{x}) \equiv 0 (\bmod p^2)} e_{p^2}(\mathbf{x} \cdot \mathbf{y}) \\
&= \sum_{Q(T(\mathbf{u})) \equiv 0 (\bmod p^2)} e_{p^2}(T(\mathbf{u}) \cdot \mathbf{y}) \\
&= \sum_{Q_1(\mathbf{u}) \equiv 0 (\bmod p^2)} e_{p^2}(\mathbf{u} \cdot T^t(\mathbf{y})) \\
&= \sum_{\mathbf{u} \in V'_{p^2}} e_{p^2}(\mathbf{u} \cdot T^t(\mathbf{y})) \\
&= \phi(V'_{p^2}, T^t(\mathbf{y})) \\
&= \phi(V'_{p^2}, \mathbf{v}).
\end{aligned}$$

Say $Q(\mathbf{x}) = \mathbf{x}^t A_Q \mathbf{x}$, where A_Q is the associated matrix for Q. Then

$$Q_1(\mathbf{u}) = Q\big(T(\mathbf{u})\big) = \big(T(\mathbf{u})\big)^t A_Q \big(T(\mathbf{u})\big) = \mathbf{u}^t \underbrace{T^t A_Q T}_{A_{Q_1}} \mathbf{u}.$$

And

$$Q_1{}^*(\mathbf{v}) = Q_1{}^*\big(T^t(\mathbf{y})\big) = \big(T^t\mathbf{y}\big)^t \left[T^{-1} A_Q^{-1} (T^t)^{-1}\right] T^t(\mathbf{y}) = \mathbf{y}^{\mathbf{t}} A_Q^{-1} \mathbf{y} = Q_1{}^*(\mathbf{y}).$$

Thus by our result for diagonal forms we have for the original quadratic form that

$$\phi(V, \mathbf{y}) = \begin{cases}
p^n - p^{n-1} & \text{if } p \nmid y_i \text{ for some } i \text{ and } p^2 \left| Q^*(\mathbf{y}), \right. \\
-p^{n-1} & \text{if } p \nmid y_i \text{ for some } i \text{ and } p \left\| Q^*(\mathbf{y}), \right. \\
0 & \text{if } p \nmid y_i \text{ for some } i \text{ and } p \nmid Q^*(\mathbf{y}), \\
-\Delta p^{(3n/2)-2} + p^{n-1}(p-1) & \text{if } p | y_i \quad \text{for all } i \text{ and } p \nmid Q^*(\mathbf{y}'), \\
\Delta(p-1)p^{(3n/2)-2} + p^{n-1}(p-1) & \text{if } p | y_i \quad \text{for all } i \text{ and } p \left| Q^*(\mathbf{y}'). \right.
\end{cases} \tag{2.7}$$

§2.3. Small solutions of the quadratic congruence $Q(\mathbf{x}) \equiv 0 \pmod{p^2}$.

We start this section by finding

2.3.1. The fundamental identity.

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

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

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

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

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

$$\sum_{\mathbf{x}\in V}\alpha(\mathbf{x}) = p^{-2}\sum_{\mathbf{x}}\alpha(\mathbf{x}) + \sum_{\mathbf{y}} a(\mathbf{y})\,\phi(V,\mathbf{y})\,, \tag{2.8}$$

because

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

Now we can prove:

Lemma 2.4. [The fundamental identity] *For any complex valued* $\alpha(\mathbf{x})$ *on* $\mathbb{Z}_{p^2}^n$

$$\begin{aligned}\sum_{\mathbf{x}\in V}\alpha(\mathbf{x}) = p^{-2}\sum_{\mathbf{x}}\alpha(\mathbf{x}) + p^n \sum_{p^2|Q^*(\mathbf{y})} a(\mathbf{y}) - p^{n-1}\sum_{p|Q^*(\mathbf{y})} a(\mathbf{y}) \\ - \Delta p^{(3n/2)-2}\sum_{\mathbf{y}'(\mathrm{mod}\,p)}^{p} a(p\mathbf{y}') + \Delta p^{(3n/2)-1}\sum_{\substack{p|Q^*(\mathbf{y}') \\ \mathbf{y}'(\mathrm{mod}\,p)}} a(p\mathbf{y}'),\end{aligned} \tag{2.9}$$

where $\mathbf{y} = p\mathbf{y}'$.

This lemma is special case of the general Lemma 4.4 of Chapter 4.

Proof. We shall use the abbreviation $\sum_{p\nmid y_i}$ to mean $\sum_{p\nmid y_i \text{ for some } i}$ and $\sum_{p|y_i}$ to mean $\sum_{p|y_i \text{ for all } i}$. Inserting (2.7) in (2.8), and simplifying, we get

$$\begin{aligned}\sum_{\mathbf{x}\in V}\alpha(\mathbf{x}) &= p^{-2}\sum_{\mathbf{x}}\alpha(\mathbf{x}) + \sum_{\mathbf{y}\,(\mathrm{mod}\,p^2)} a(\mathbf{y})\,\phi(V,\mathbf{y}) \\ &= p^{-2}\sum_{\mathbf{x}}\alpha(\mathbf{x}) + \underbrace{\sum_{p\nmid y_i,\ p^2|Q^*(\mathbf{y})} \left(p^n - p^{n-1}\right) a(\mathbf{y})}_{T_1} - \underbrace{\sum_{p\nmid y_i,\ p\|Q^*(\mathbf{y})} p^{n-1}a(\mathbf{y})}_{T_2} \\ &\qquad + \underbrace{\sum_{p|y_i,\ p\nmid Q^*(\mathbf{y}')} \left(-\Delta p^{(3n/2)-2} + p^{n-1}(p-1)\right)a(\mathbf{y})}_{T_3} \\ &\qquad + \underbrace{\sum_{p|y_i,\ p\,|Q^*(\mathbf{y}')} \left(\Delta(p-1)p^{(3n/2)-2} + p^{n-1}(p-1)\right)a(\mathbf{y})}_{T_4}.\end{aligned}$$

Next, denote

$$T = T_1 + T_2 + T_3 + T_4.$$

Then after some manipulation, T reduces to

$$\begin{aligned}T = (p^n - p^{n-1}) &\sum_{p^2|Q^*(\mathbf{y})} a(\mathbf{y}) - \Delta p^{(3n/2)-2}\sum_{p|y_i} a(\mathbf{y}) \\ &- p^{n-1}\sum_{p\nmid y_i,\ p\|Q^*(\mathbf{y})} a(\mathbf{y}) + \Delta p^{(3n/2)-1}\sum_{p|y_i,\ p|Q^*(y')} a(\mathbf{y}).\end{aligned} \tag{2.10}$$

Now, we note that in (2.10) the sum

$$-p^{n-1}\sum_{p\nmid y_i,\ p\|Q^*(\mathbf{y})} a(\mathbf{y}) = -p^{n-1}\Bigg(\sum_{p\nmid y_i,\ p|Q^*(\mathbf{y})} a(\mathbf{y}) - \sum_{p\nmid y_i,\ p^2|Q^*(\mathbf{y})} a(\mathbf{y})\Bigg). \tag{2.11}$$

On the other hand, we observe that in (2.11) the sum

$$p^{n-1}\sum_{p\nmid y_i,\ p^2|Q^*(\mathbf{y})} a(\mathbf{y}) = p^{n-1}\Bigg(\sum_{p^2|Q^*(\mathbf{y})} a(\mathbf{y}) - \sum_{p|y_i} a(\mathbf{y})\Bigg), \tag{2.12}$$

and the sum

$$-p^{n-1}\sum_{p\nmid y_i,\ p|Q^*(\mathbf{y})} a(\mathbf{y}) = -p^{n-1}\Bigg(\sum_{p|Q^*(\mathbf{y})} a(\mathbf{y}) - \sum_{p|y_i} a(\mathbf{y})\Bigg). \tag{2.13}$$

So, by using (2.12) and (2.13), the sum (2.11) becomes

$$-p^{n-1}\sum_{p\nmid y_i,\ p\|Q^*(\mathbf{y})} a(\mathbf{y}) = p^{n-1}\sum_{p^2|Q^*(\mathbf{y})} a(\mathbf{y}) - p^{n-1}\sum_{p|Q^*(\mathbf{y})} a(\mathbf{y}). \tag{2.14}$$

Consequently, by using (2.14), (2.10) becomes

$$\begin{aligned} T &= p^n \sum_{p^2|Q^*(\mathbf{y})} a(\mathbf{y}) - p^{n-1}\sum_{p^2|Q^*(\mathbf{y})} a(\mathbf{y}) - \Delta p^{(3n/2)-2}\sum_{y_i'=1}^{p} a(p\mathbf{y}') \\ &\qquad + p^{n-1}\sum_{p^2|Q^*(\mathbf{y})} a(\mathbf{y}) - p^{n-1}\sum_{p|Q^*(\mathbf{y})} a(\mathbf{y}) + \Delta p^{(3n/2)-1}\sum_{\substack{y_i'=1 \\ p|Q^*(\mathbf{y}')}}^{p} a(p\mathbf{y}') \\ &= p^n \sum_{p^2|Q^*(\mathbf{y})} a(\mathbf{y}) - \Delta p^{(3n/2)-2}\sum_{y_i'=1}^{p} a(p\mathbf{y}') \\ &\qquad - p^{n-1}\sum_{p|Q^*(\mathbf{y})} a(\mathbf{y}) + \Delta p^{(3n/2)-1}\sum_{p|Q^*(\mathbf{y}')} a(p\mathbf{y}'). \end{aligned}$$

Hence, it follows that

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

which is the assertion of Lemma 2.4. □

2.3.2. Upper bounds on $\left|\mathscr{B}\cap V_p\right|$.

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

$$\mathscr{B} = \left\{\mathbf{x}\in\mathbb{Z}^n \,\middle|\, a_i \le x_i < a_i + m_i,\ 1\le i\le n\right\}, \tag{2.15}$$

where $m_i = q_i p + r_i,\ 0\le r_i < p$ and $q_i, r_i \in \mathbb{Z}$. Thus the number of points in $\mathscr{B}$ (cardinality of $\mathscr{B}$) is $|\mathscr{B}| = \prod_{i=1}^n m_i$. Our interst in this section is determining the number of solutions of

$$Q(\mathbf{x}) \equiv 0 \pmod p, \tag{2.16}$$

with $x\in\mathscr{B}$. First we treat the case where all $m_i \le p$. In this case we can view the box $\mathscr{B}$ in (2.15) as a subset of $\mathbb{Z}_p^n$ and let $\chi_{\mathscr{B}}$ be its characteristic function with Fourier expansion $\chi_{\mathscr{B}}(\mathbf{x}) = \sum_{\mathbf{y}} a_{\mathscr{B}}(\mathbf{y}) e_p(\mathbf{x}\cdot\mathbf{y})$. Then for any $\mathbf{y}\in\mathbb{Z}_p^n$,

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

and so (by work of [**12**]),

$$\sum_{\mathbf{y}}\left|a_{\mathscr{B}}(\mathbf{y})\right| \le \prod_{i=1}^{n}\frac{1}{p}\left|\sum_{\mathbf{y}}\frac{\sin(\pi m_i y/p)}{\sin(\pi y/p)}\right| \le \left(\frac{4}{\pi^2}\log p+1\right)^n \le \left(\frac{4}{\pi^2}\log(12p)\right)^n. \tag{2.17}$$

Lemma 2.5. *Let* $\mathscr{B}$ *be a box of type* (2.15) *centered at the origin with all* $m_i \le p$, *and* $V_p = V_p(Q)$ *denote to the set of solutions of* (2.16) *in* $\mathbb{Z}_p^n$. *If* $\Delta_Q = +1$, *then*

a) $$\left|\mathscr{B}\bigcap V_p\right| \le \frac{|\mathscr{B}|}{p} + p^{n/2}\left(\frac{4}{\pi^2}\log(12p)\right)^n. \tag{2.18}$$

b) $$\left|\mathscr{B}\bigcap V_p\right| \le 2^n\left(\frac{|\mathscr{B}|}{p} + p^{n/2}\right). \tag{2.19}$$

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

$$\sum_{\mathbf{x}\in V_p}\alpha(\mathbf{x}) = p^{-1}\sum_{\mathbf{x}}\alpha(\mathbf{x}) - \alpha(\mathbf{0})p^{n/2-1} + p^{n/2}\sum_{Q^*(\mathbf{y})=\mathbf{0}}a(\mathbf{y}), \tag{2.20}$$

by Lemma 1.2 of Chapter 1. Letting $\alpha(\mathbf{x}) = \chi_{\mathscr{B}}(\mathbf{x}) = \sum_{\mathbf{y}} a_{\mathscr{B}}(\mathbf{y})e_p(\mathbf{x}\cdot\mathbf{y})$, in (2.20), we have

$$\sum_{\mathbf{x}\in V_p}\chi_{\mathscr{B}}(\mathbf{x}) \le \frac{|\mathscr{B}|}{p} + p^{n/2}\sum_{\mathbf{y}}\left|a_{\mathscr{B}}(\mathbf{y})\right|,$$

and so (using 2.17),

$$\left|\mathscr{B}\bigcap V_p\right| \le \frac{|\mathscr{B}|}{p} + p^{n/2}\left(\frac{4}{\pi^2}\log(12p)\right)^n,$$

completing the proof of part (a). For part (b) set $\alpha = \chi_{\mathscr{B}} * \chi_{\mathscr{B}}$, the convolution of $\chi_{\mathscr{B}}$ with itself, i.e.;

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

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

((1.10), Chapter 1),

$$\sum_{\mathbf{y}}\left|a(\mathbf{y})\right| = p^{n}\sum_{\mathbf{y}}\left|a_{\mathscr{B}}(\mathbf{y})\right|^{2} = \sum_{\mathbf{y}}\chi^{2}_{\mathscr{B}}(\mathbf{y}) = |\mathscr{B}|. \tag{2.21}$$

Also Next by (2.20), we observe that

$$\begin{aligned}\sum_{\mathbf{x}\in V_p}\alpha(\mathbf{x}) &\le p^{-1}\sum_{\mathbf{x}}\alpha(\mathbf{x}) + p^{n/2}\sum_{\mathbf{y}}a(\mathbf{y})\\ &= p^{-1}\sum_{\mathbf{x}}(\chi_{\mathscr{B}} * \chi_{\mathscr{B}})(\mathbf{x}) + p^{n/2}\sum_{\mathbf{y}}\left|a(\mathbf{y})\right|.\end{aligned}$$

Then, using the identity ((1.9), Chapter 1) and (2.21), the above is

$$\begin{aligned}\sum_{\mathbf{x}\in V_p}\alpha(\mathbf{x}) &\le p^{-1}\left[\Big(\sum_{\mathbf{u}}\chi_{\mathscr{B}}(\mathbf{u})\Big)\cdot\Big(\sum_{\mathbf{v}}\chi_{\mathscr{B}}(\mathbf{v})\Big)\right] + p^{n/2}\,|\mathscr{B}|\\ &= p^{-1}\,|\mathscr{B}|\,|\mathscr{B}\,| + p^{n/2}\,|\mathscr{B}|\\ &= \frac{|\mathscr{B}|^{2}}{p} + p^{n/2}\,|\mathscr{B}|,\end{aligned} \tag{2.22}$$

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

$$\alpha(\mathbf{x}) = \chi_{\mathscr{B}} * \chi_{\mathscr{B}}(\mathbf{x}) \ge 2^{-n}\,|\mathscr{B}|. \tag{2.23}$$

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 $x\in I$,

$$\chi_I * \chi_I(x) \ge \frac{1}{2}|I| = \frac{1}{2}(2M+1). \tag{2.24}$$

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 $-M\le x\le 0$, then the number of points is $2M+x+1$, specifically $x=u+(x-u)$, $-M\le u\le x+M$. Thus plainly the total number of the points is greater than or equal to

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

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

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

The two cases imply (2.24). Thus it follows immediately that for $x\in I_1\times\ldots\times I_n = \mathscr{B}$,

$$\alpha(\mathbf{x}) = \prod_{i=1}^{n} \chi_{I_i} * \chi_{I_i}(\mathbf{x}) \underset{\text{by (2.24)}}{\geq} \prod_{i=1}^{n} \frac{1}{2}|I_i| = 2^{-n}\,|\mathscr{B}|,$$

which is (2.23). Now we return to complete proving the lemma. From (2.23) it follows that

$$\sum_{\mathbf{x}\in V_p} \alpha(\mathbf{x}) \geq \sum_{\mathbf{x}\in V_p \cap \mathscr{B}} 2^{-n}\,|\mathscr{B}| = 2^{-n}\,|\mathscr{B}|\big|\mathscr{B} \bigcap V_p\big|. \tag{2.25}$$

Thus, putting (2.22) and (2.25) together and simplifying we conclude that

$$\big|\mathscr{B} \bigcap V_p\big| \leq 2^n\Big(\frac{|\mathscr{B}|}{p} + p^{n/2}\Big).$$

The lemma is thereby proved. □

Lemma 2.5 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 2.6. *Let* $\mathscr{B}$ *be any box of type* (2.15) *with all* $m_i \leq p$, *and* $V_p = V_p(Q)$ *denote to the set of solutions of* (2.16) *in* $\mathbb{Z}_p^n$. *If* $\Delta_Q = +1$, *then*

$$\big|\mathscr{B} \bigcap V_p\big| \leq 2^n\Big(\frac{|\mathscr{B}|}{p} + p^{n/2}\Big). \tag{2.26}$$

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

$$\sum_{\mathbf{x}\in V_p} \alpha(\mathbf{x}) = p^{-1}\sum_{\mathbf{x}} \alpha(\mathbf{x}) - \alpha(\mathbf{0})p^{n/2-1} + p^{n/2} \sum_{Q^*(\mathbf{y})=\mathbf{0}} a(\mathbf{y}). \tag{2.27}$$

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

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

Then

$$\sum_{\mathbf{x}} \alpha(\mathbf{x}) = |\mathscr{B}||\mathscr{B}'| = |\mathscr{B}|^2, \tag{2.28}$$

$$\alpha(\mathbf{0}) = \sum_{\substack{u\in\mathscr{B} \\ \mathbf{u}+\mathbf{v}=\mathbf{0}}} \sum_{v\in\mathscr{B}'} 1 \leq |\mathscr{B}|, \tag{2.29}$$

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

Thus, using the Cauchy-Schwartz inequality (see e.g. [**28**]) and Parseval's identity, (1.10) of Chapter 1, we obtain

$$\begin{aligned}
\sum_{\mathbf{y}} \big|a(\mathbf{y})\big| &= p^n \sum_{\mathbf{y}} \Big|a_{\mathscr{B}}(\mathbf{y})\, a_{\mathscr{B}'}(\mathbf{y})\Big| \\
&\le p^n \Big(\sum_{\mathbf{y}} \big|a_{\mathscr{B}}(\mathbf{y})\big|^2\Big)^{1/2} \Big(\sum_{\mathbf{y}'} \big|a_{\mathscr{B}'}(\mathbf{y}')\big|^2\Big)^{1/2} \\
&\le p^n \Big(\frac{1}{p^n} \sum_{\mathbf{y}} \chi^2_{\mathscr{B}}(\mathbf{x})\Big)^{1/2} \Big(\frac{1}{p^n} \sum_{\mathbf{y}} \chi^2_{\mathscr{B}'}(\mathbf{x})\Big)^{1/2} \\
&= |\mathscr{B}|^{1/2} \big|\mathscr{B}'\big|^{1/2} = |\mathscr{B}|. \qquad (2.30)
\end{aligned}$$

Thus by the fundamental identity (2.27) and (2.28), (2.29), and (2.30), if $\Delta = +1$,

$$\begin{aligned}
\sum_{\mathbf{x}\in V_p} \alpha(\mathbf{x}) &\le p^{-1} \sum_{\mathbf{x}} \alpha(\mathbf{x}) + p^{n/2} \sum_{\substack{\mathbf{y} \\ Q^*(\mathbf{y})=0}} \big|a(\mathbf{y})\big| \\
&\le p^{-1} \sum_{\mathbf{x}} \alpha(\mathbf{x}) + p^{n/2} \sum_{\mathbf{y}} \big|a(\mathbf{y})\big| \\
&\le \frac{|\mathscr{B}|^2}{p} + p^{n/2}\, |\mathscr{B}|. \qquad (2.31)
\end{aligned}$$

Now we claim that

$$\sum_{\mathbf{x}\in V_p} \alpha(\mathbf{x}) \ge \sum_{\mathbf{x}\in V_p \cap \mathscr{B}} 2^{-n}\, |\mathscr{B}| = 2^{-n}\, |\mathscr{B}| \big|V_p \cap \mathscr{B}\big|. \qquad (2.32)$$

To see (2.32), we are going to argue as follows. Let

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

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

$$I' = I - c_i = \Big\{-\frac{m_i - 1}{2}, \ldots, \frac{m_i - 1}{2}\Big\}.$$

Thus for any $x \in I$,

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

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

$$I' = I - c_i = \Big\{-\frac{m_i}{2} + 1, \ldots, \frac{m_i}{2}\Big\}.$$

Hence for any $x \in I$,

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

So

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

and the claim follows. Now we combine (2.31) and (2.32), we get

$$\left|\mathscr{B} \bigcap V_p\right| \leq 2^n\left(\frac{|\mathscr{B}|}{p} + p^{n/2}\right),$$

which completes the proof of Lemma 2.6. □

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

$$N_{\mathscr{B}} = \prod_{i=1}^{n}\left(\left[\frac{m_i}{p}\right]+1\right). \tag{2.33}$$

Lemma 2.7. *Let $V_{p,\mathbb{Z}} = V_{p,\mathbb{Z}}(Q)$ be the set of integer solutions of the congruence* (2.16) *and let $\Delta_p = 1$. Then for any box $\mathscr{B}$ of type* (2.15),

$$\left|\mathscr{B} \bigcap V_{p,\mathbb{Z}}\right| \leq 2^n\left(\frac{|\mathscr{B}|}{p} + N_{\mathscr{B}}\ p^{n/2}\right). \tag{2.34}$$

Proof. Partition $\mathscr{B}$ into $N = N_{\mathscr{B}}$ smaller boxes B_i,

$$\mathscr{B} = B_1 \bigcup B_2 \bigcup \cdots \bigcup B_N,$$

where each B_i has all of its edge lengths $\leq p$. Thus Lemma 2.6 can be applied to each B_i. We obtain

$$\begin{aligned}
\left|\mathscr{B} \bigcap V_{p,\mathbb{Z}}\right| &= \sum_{i=1}^{N}\left|\, B_i \bigcap V_p \,\right| \\
&\overset{\text{(Lemma 2.6)}}{\uparrow} \leq \sum_{i=1}^{N} 2^n\left(\frac{|B_i|}{p} + p^{n/2}\right) \\
&= \frac{2^n}{p}\sum_{i=1}^{N}|B_i| + N2^n p^{n/2} \\
&= 2^n\left(\frac{|\mathscr{B}|}{p} + N\ p^{n/2}\right).
\end{aligned}$$

So the proof of Lemma 2.7 is complete. □

2.3.3. Bounds on the error terms in the fundamental identity modulo p^2 when $\Delta = +1$.

Let $\mathscr{B}$ be a box of points in $\mathbb{Z}^n$ as in (2.15) 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 $\chi_{\mathscr{B}}$ be its characteristic function with Fourier expansion $\chi_{\mathscr{B}}(\mathbf{x}) = \sum_{\mathbf{y}} a_{\mathscr{B}}(\mathbf{y}) e_{p^2}(\mathbf{x}\cdot\mathbf{y})$. Let $\alpha(\mathbf{x}) = \chi_{\mathscr{B}} * \chi_{\mathscr{B}} = \sum_{\mathbf{y}} a(\mathbf{y}) e_{p^2}(\mathbf{x}\cdot\mathbf{y})$. Then for any $\mathbf{y} \in \mathbb{Z}_{p^2}^n$,

$$a(\mathbf{y}) = p^{-2n} \prod_{i=1}^{n} \frac{\sin^2 \pi m_i y_i / p^2}{\sin^2 \pi y_i / p^2}, \tag{2.35}$$

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,

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

Suppose $\mathscr{B}$ is centered about the origin. If $\Delta = +1$, then we apply the fundamental identity (2.9) to $\alpha(\mathbf{x}) = \chi_{\mathscr{B}} * \chi_{\mathscr{B}}$ to get

$$\begin{aligned} \sum_{\mathbf{x}\in V} \alpha(\mathbf{x}) &\ge \underbrace{p^{-2} \sum_{\mathbf{x}} \alpha(\mathbf{x})}_{\text{Main Term}} - \underbrace{p^{n-1} \sum_{p \mid Q^*(\mathbf{y})} a(\mathbf{y})}_{E_1} - \underbrace{p^{(3n/2)-2} \sum_{\mathbf{y} \,(\mathrm{mod}\, p)} a(p\mathbf{y})}_{E_2} \\ &\ge Main\ \ Term - E_1 - E_2, \end{aligned} \tag{2.36}$$

since our box $\mathscr{B}$ is centered about the origin, and so the Fourier coefficients $a(\mathbf{y})$ are all positive. The main term in (2.36) is

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

and the others are error terms. We proceed to bound these error terms. We shall, in this section and next, refer to any error term or to the value which bounded that error term by E_i or E_{ij}, $i, j \in \{1,2,3,4\}$. For the error term E_1 we first observe

$$E_1 = p^{n-1} \sum_{Q^*(\mathbf{y}) \equiv 0 \,(\mathrm{mod}\, p)} a(\mathbf{y}) \le p^{n-1} \sum_{Q^*(\mathbf{y}) \equiv 0 \,(\mathrm{mod}\, p)} \left| a(\mathbf{y}) \right|. \tag{2.37}$$

Then it is clear now we only need to bound the sum $\sum_{Q^*(\mathbf{y}) \equiv 0 \bmod p} \left| a(\mathbf{y}) \right|$. Let $\sum^*$ be an abbreviation for $\sum_{Q^*(\mathbf{y}) \equiv 0 (\mathrm{mod}\, p), |y_i| < p^2/2}$. Define ρ_i by

$$\rho_i = \begin{cases} 2^{k_i-1} & \text{for } k_i \geq 1, \\ 0 & \text{for } k_i = 0. \end{cases} \tag{2.38}$$

Using the fact that

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

yields

$$\begin{aligned} \sum_{\substack{Q^*(\mathbf{y}) \equiv 0 (\mathrm{mod}\, p) \\ |y_i| \leq p^2/2}} \left|a(\mathbf{y})\right| &\leq \sum_{k_1=0}^{\infty} \cdots \sum_{k_n=0}^{\infty} \sum_{\substack{\mathbf{y} \\ \rho_i p^2/m_i \leq |y_i| \leq 2^{k_i} p^2/m_i}}^{*} \prod_{i=1}^{n} \min\left\{ \frac{m_i^2}{p^2}, \frac{p^2}{4y_i^2} \right\} \\ &\leq \sum_{k_1=0}^{\infty} \cdots \sum_{k_n=0}^{\infty} \sum_{\substack{\mathbf{y} \\ |y_i| \leq 2^{k_i} p^2/m_i}}^{*} \prod_{i=1}^{n} \frac{p^2}{4(2^{k_i-1} p^2/m_i)^2}. \\ &= \frac{|\mathscr{B}|^2}{p^{2n}} \sum_{k_1=0}^{\infty} \cdots \sum_{k_n=0}^{\infty} \sum_{\substack{\mathbf{y} \\ |y_i| \leq 2^{k_i} p^2/m_i}}^{*} \prod_{i=1}^{n} \frac{1}{2^{2k_i}}. \end{aligned} \tag{2.39}$$

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

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

Put

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

so that

$$|\mathscr{B}'| = \prod_{i=1}^{n} m_i' \leq \prod_{i=1}^{n} \left(\frac{2^{k_i+1} p^2}{m_i} + 1 \right) \leq \prod_{i=1}^{n} \frac{2^{k_i+2} p^2}{m_i} = 4^n \frac{p^{2n}}{|\mathscr{B}|} \prod_{i=1}^{n} 2^{k_i}. \tag{2.40}$$

Now, from the upper bound (2.34), we have

$$\left| \mathscr{B}' \bigcap V_{p,\mathbb{Z}} \right| \leq 2^n \frac{|\mathscr{B}'|}{p} + 2^n N_{\mathscr{B}'}\, p^{n/2}, \tag{2.41}$$

where by utilizing (2.33),

$$N_{\mathscr{B}'} = \prod_{i=1}^{n} \left(\left\lfloor \frac{m_i'}{p} \right\rfloor + 1 \right) = \prod_{2^{k_i} \geq m_i/4p}^{n} \left(\left\lfloor \frac{m_i'}{p} \right\rfloor + 1 \right). \tag{2.42}$$

The last equality in (2.42) follows, since

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

But the right -hand side of (2.42), is less than or equal to

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

It follows that

$$N_{\mathscr{B}'}\leq 2^n\prod_{\substack{i=1\\ 2^{k_i}\geq m_i/4p}}^{n}\left(\frac{2^{k_i}p}{m_i}+1\right). \tag{2.43}$$

Apply the upper bound (2.41) to the inner sum $\sum_{\mathbf{y}}^{*}$ in (2.39). This gives

$$\begin{aligned}\sum_{\substack{Q^*(\mathbf{y})\equiv 0(\mathrm{mod}\,p)\\ |y_i|\leq p^2/2}}\left|a(\mathbf{y})\right| &\leq \frac{|\mathscr{B}|^2}{p^{2n}}\sum_{k_1=0}^{\infty}\cdots\sum_{k_n=0}^{\infty}\left|\mathscr{B}'\cap V_{p,\mathbb{Z}}\right|\prod_{i=1}^{n}\frac{1}{2^{2k_i}}\\ &\leq \frac{|\mathscr{B}|^2}{p^{2n}}\sum_{k_1=0}^{\infty}\cdots\sum_{k_n=0}^{\infty}\left(2^n\,\frac{|\mathscr{B}'|}{p}+2^n N_{\mathscr{B}'}\;p^{n/2}\right)\prod_{i=1}^{n}\frac{1}{2^{2k_i}}\\ &\leq \sigma_1+\sigma_2, \end{aligned}\tag{2.44}$$

where by employing the inequality (2.40), we find that

$$\begin{aligned}\sigma_1 &= \frac{|\mathscr{B}|^2}{p^{2n}}\sum_{k_1=0}^{\infty}\cdots\sum_{k_n=0}^{\infty}\left(\prod_{i=1}^{n}\frac{1}{2^{2k_i}}\right)\frac{2^n\,|\mathscr{B}'|}{p}\\ &\leq \frac{|\mathscr{B}|^2}{p^{2n}}\sum_{k_1=0}^{\infty}\cdots\sum_{k_n=0}^{\infty}\left(\prod_{i=1}^{n}\frac{1}{2^{2k_i}}\right)\left(\frac{2^n}{p}\,4^n\,\frac{p^{2n}}{|\mathscr{B}|}\prod_{i=1}^{n}2^{k_i}\right)\\ &= 8^n\,\frac{|\mathscr{B}|}{p}\sum_{k_1=0}^{\infty}\cdots\sum_{k_n=0}^{\infty}\left(\prod_{i=1}^{n}\frac{1}{2^{k_i}}\right)\\ &\leq 8^n\cdot 2^n\,\frac{|\mathscr{B}|}{p}=16^n\,\frac{|\mathscr{B}|}{p}, \end{aligned}\tag{2.45}$$

and by the inequality (2.43),

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

$$
\begin{aligned}
&= \frac{4^n\,|\mathscr{B}|^2}{p^{3n/2}} \prod_{i=1}^{n} \left[\sum_{k_i=0}^{\infty} \frac{1}{2^{2k_i}} + \sum_{\substack{k_i \\ 2^{k_i} \geq m_i/4p}} \frac{p}{2^{k_i} m_i} \right] \\
&= \frac{4^n\,|\mathscr{B}|^2}{p^{3n/2}} \prod_{i=1}^{n} \left[\frac{4}{3} + \frac{p}{m_i} \sum_{\substack{k_i=0 \\ 2^{k_i} \geq m_i/4p}}^{\infty} \frac{1}{2^{k_i}} \right], \\
&\leq \frac{4^n\,|\mathscr{B}|^2}{p^{3n/2}} \prod_{i=1}^{n} \left[\frac{4}{3} + \min\left(\frac{2p}{m_i}, \frac{8p^2}{m_i^2} \right) \right]. \qquad (2.46)
\end{aligned}
$$

Thus by inequalities (2.37), (2.44), (2.45) and (2.46), we have

$$
\begin{aligned}
E_1 &\leq 16^n\,\frac{|\mathscr{B}|}{p}\,p^{n-1} + \frac{4^n\,|\mathscr{B}|^2}{p^{3n/2}}\,p^{n-1} \prod_{i=1}^{n} \left[\frac{4}{3} + \min\left(\frac{2p}{m_i}, \frac{8p^2}{m_i^2} \right) \right] \\
&= \underbrace{2^{4n}\,p^{n-2}\,|\mathscr{B}|}_{E_{1,1}} + \underbrace{\frac{4^n\,|\mathscr{B}|^2}{p^{n/2+1}} \prod_{i=1}^{n} \left[\frac{4}{3} + \min\left(\frac{2p}{m_i}, \frac{8p^2}{m_i^2} \right) \right]}_{E_{1,2}}. \qquad (2.47)
\end{aligned}
$$

Now assume that

$$
m_1 \leq \cdots \leq m_l \leq p < m_{l+1} \leq \cdots \leq m_n\,. \qquad (2.48)
$$

Then for $m_i \leq p$,

$$
\frac{4}{3} + \min\left(\frac{2p}{m_i}, 8\Big(\frac{p}{m_i}\Big)^2 \right) \leq \frac{4}{3} + \frac{2p}{m_i} \leq \frac{4p}{m_i}, \qquad (2.49)
$$

and for $m_i > p$,

$$
\frac{4}{3} + \min\left(\frac{2p}{m_i}, 8\Big(\frac{p}{m_i}\Big)^2 \right) \leq \frac{4}{3} + 2 \leq \frac{10}{3}. \qquad (2.50)
$$

By (2.49) and (2.50), we can write

$$
\prod_{i=1}^{n} \left[\frac{4}{3} + \min\left(\frac{2p}{m_i}, \frac{8p^2}{m_i^2} \right) \right] \leq \prod_{i=1}^{l} \frac{4p}{m_i} \cdot \prod_{i=l+1}^{n} \frac{10}{3} = \frac{4^l\,p^l}{\prod_{i=1}^{l} m_i} \Big(\frac{10}{3}\Big)^{n-l} \leq \frac{4^n\,p^l}{\prod_{i=1}^{l} m_i}, \qquad (2.51)
$$

and consequently (using (2.47) and (2.51))

$$
\begin{aligned}
E_{1,2} &\leq \frac{4^n\,|\mathscr{B}|^2}{p^{n/2+1}} \frac{4^n\,p^l}{\prod_{i=1}^{l} m_i} \\
&= \frac{2^{4n} \prod_{i=1}^{n} m_i^2}{p^{n/2-l+1} \cdot \prod_{i=1}^{l} m_i} \\
&= 2^{4n}\,p^{l-(n/2)-1} \prod_{i=1}^{n} m_i \prod_{i=l+1}^{n} m_i \\
&= 2^{4n}\,p^{l-(n/2)-1}\,|\mathscr{B}| \prod_{i=l+1}^{n} m_i. \qquad (2.52)
\end{aligned}
$$

Therefore by inequalities (2.47) and (2.52), we arrive at

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

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

Lemma 2.8. Let $\mathscr{B}$ be any box of type (2.15) and $\alpha(\mathbf{x}) = \chi_{\mathscr{B}} * \chi_{\mathscr{B}}(\mathbf{x})$. Suppose

$$m_1 \le m_2 \le \cdots \le m_l < p \le m_{l+1} \le \cdots \le m_n. \tag{2.53}$$

Then we have

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

Proof. We first observe,

$$\begin{aligned}
\sum_{y=1}^{p} a(p\mathbf{y}) &= \sum_{y_i=1}^{p} \sum_{x_i=1}^{p^2} \frac{1}{p^{2n}} \alpha(\mathbf{x}) e_{p^2}(-\mathbf{x} \cdot p\mathbf{y}) \\
&= \sum_{x_i=1}^{p^2} \frac{1}{p^{2n}} \alpha(\mathbf{x}) \sum_{y_i=1}^{p} e_p(-\mathbf{x} \cdot \mathbf{y}) \\
&= \sum_{\substack{x_i=1 \\ \mathbf{x} \equiv 0 \,(\mathrm{mod}\, p)}}^{p^2} \frac{p^n}{p^{2n}} \alpha(\mathbf{x}) \\
&= \frac{1}{p^n} \sum_{\mathbf{x} \equiv 0 \,(\mathrm{mod}\, p)} \alpha(\mathbf{x}) \\
&= \frac{1}{p^n} \sum_{\substack{\mathbf{u} \in \mathscr{B} \\ \mathbf{u}+\mathbf{v} \equiv 0 (\mathrm{mod}\, p)}} \sum_{\mathbf{v} \in \mathscr{B}} 1 \\
&\le \frac{1}{p^n} \prod_{i=1}^{n} m_i \left(\left[\frac{m_i}{p} \right] + 1 \right).
\end{aligned} \tag{2.54}$$

To obtain the last inequality in (2.54) we must count the number of solutions of the congruence

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

with $\mathbf{u}, \mathbf{v} \in \mathscr{B}$. 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 (2.53) then continuing from (2.54) we have

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

The lemma is established. □

Now in view of Lemma 2.8, it is clear that the error term E_2 has the estimate

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

The following theorem summarizes the final outcome of our investigation for the error terms in the case of $\Delta = +1$.

Theorem 2.2. *Suppose that $n \ge 4$ is even, and that $\Delta_p(Q) = +1$. Then for any box $\mathscr{B}$ centered at the origin,*

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

where

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

In Theorem 2.2 we have indicated below each term, the error term bounded by the given value.

Next we compare each error term in Theorem 2.2 to the main term $|\mathscr{B}|^2 / p^2$. To make the left-hand side greater than $1/4$ of the main term, we make each error term less than $1/4$ of the main term. For the error term $E_{1,1}$, we need

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

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

$$\begin{aligned} & \frac{1}{4}\frac{|\mathscr{B}|^2}{p^2} \geq 2^{4n}\, p^{l-(n/2)-1}\, |\mathscr{B}| \prod_{i=l+1}^{n} m_i \\ \iff \qquad & \prod_{i=1}^{l} m_i \geq 2^{4n+2}\, p^{l-(n/2)+1} \\ \iff \qquad & \prod_{i=1}^{l} \frac{p}{m_i} \leq 2^{-4n-2}\, p^{(n/2)-1}. \end{aligned}$$

Finally for the error term E_2,

$$\begin{aligned} & \frac{1}{4}\frac{|\mathscr{B}|^2}{p^2} \geq 2^{n-l}\, p^{l-(n/2)-2}\, |\mathscr{B}| \prod_{i=l+1}^{n} m_i \\ \iff \qquad & |\mathscr{B}| \geq 4 \cdot 2^{n-l}\, p^{l-(n/2)} \prod_{i=l+1}^{n} m_i \\ \iff \qquad & \prod_{i=1}^{l} \frac{p}{m_i} \leq 2^{l-n-2}\, p^{n/2}. \end{aligned}$$

Putting the pieces together, we deduce

Theorem 2.3. *Suppose that* $n \geq 4$ *is even, and that* $\Delta_p(Q) = +1$. *If* $|\mathscr{B}| \geq 2^{4n+2}\, p^n$ *and* $\prod_{i=1}^{l}(p/m_i) \leq 2^{-4n-2}\, p^{(n/2)-1}$ (*where L.H.S* $= 1$ *if* $l = 0$), *then*

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

In particular

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

Recall that a solution of (2.1) is called primitive if some coordinate is ***not*** divisible by p, i.e.; $p \nmid x_i$ for some i. We write $p|\mathbf{x}$ for imprimitive points. In fact

Corollary 2.1. *Under the hypotheses of Theorem* 2.3, $\mathscr{B} + \mathscr{B}$ *contains a primitive solution of* (2.1).

Proof. We need to show that

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

First by Lemma 2.8,

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

The last inequality is guaranteed by our hypothesis (Theorem 2.3) that

$$\prod_{i=1}^{l}\frac{p}{m_i} \le 2^{-4n-2}\,p^{(n/2)-1}. \tag{2.55}$$

More precisely, assume (2.55), then certainly

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

So we have now on the one hand,

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

On the other hand, by Theorem 2.3, we have

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

We therefore get

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

The proof of the Corollary is complete. □

Now we complete the picture by proving the following special cases.

Corollary 2.2. *Let* $\Delta_p(Q)=1$ *and let* $\mathscr{B}$ *be a cube centered at the origin with all* $m_i = B$, $B > 2^{4+(2/n)}p$, *and* $p \ge 2^{(8n+4)/(n-2)}$. *Then* $\mathscr{B}+\mathscr{B}$

contains a primitive solution of (2.1).

Proof. Suppose that $B > 2^{4+(2/n)}p$ and $p \geq 2^{(8n+4)/(n-2)}$. Then $l = 0$ and the hypotheses of Corollary 2.1 are satisfied. □

Corollary 2.3. *Let* $\mathscr{B}$ *be a rectangular box centered at the origin with*

$$m_1 = \cdots = m_l = 1, \;\; m_{l+1} = \cdots = m_n \geq 2^{(4n+2)/(n-l)} p^{n/(n-l)},$$

for some $l \leq (n/2) - 2$ *and*

$$p \geq 2^{4(2n+1)/(n-2l-2)}.$$

Then $\mathscr{B} + \mathscr{B}$ *contains primitive solution* (2.1).

Proof. Suppose that the hypotheses of Corollary 2.3 hold. Then we have that

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

Also,

$$|\mathscr{B}| \geq 2^{(4n+2)(n-l)/(n-l)} p^{n(n-l)/(n-l)} = 2^{(4n+2)} p^n.$$

So Corollary 2.1 applies. □

2.3.4. Bounds on the error terms in the fundamental identity modulo p^2 when $\Delta = -1$.

In this subsection we focus our work on the case $\Delta = -1$. Again we consider the case of a box $\mathscr{B}$ symmetric about the origin. We start by noticing that Lemma 2.6 could be rewritten in this case as follows:

Lemma 2.9. *Let* $\mathscr{B}$ *be any box of type* (2.15) *with all* $m_i \leq p$, *and* $V_p = V_p(Q)$ *denote to the set of solutions of* (2.16) *in* $\mathbb{Z}_p^n$. *If* $\Delta_p = -1$, *then*

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

Proof. The proof is similar to the proof of Lemma 2.6. The fundamental identity modulo p when $\Delta_p = -1$ is given by

$$\sum_{\mathbf{x} \in V_p} \alpha(\mathbf{x}) = p^{-1} \sum_{\mathbf{x}} \alpha(\mathbf{x}) + \alpha(\mathbf{0}) p^{n/2-1} - p^{n/2} \sum_{Q^*(\mathbf{y})=0} a(\mathbf{y}). \qquad (2.56)$$

Let α be as given in the proof of Lemma 2.6. By (2.56),(2.28),(2.29) and (2.30),

$$\begin{aligned}\sum_{\mathbf{x}\in V_p}\alpha(\mathbf{x}) &\le \frac{|\mathscr{B}|^2}{p} + p^{(n/2)-1}\,|\mathscr{B}| + p^{n/2}\sum_{\mathbf{y}}|a(\mathbf{y})| \\ &\le \frac{|\mathscr{B}|^2}{p} + p^{n/2}\,|\mathscr{B}|\Big(\frac{1}{p}+1\Big) \\ &\le \frac{|\mathscr{B}|^2}{p} + 2p^{n/2}\,|\mathscr{B}|.\end{aligned}$$

But, in the proof of Lemma 2.6, we proved that

$$\sum_{\mathbf{x}\in V_p}\alpha(\mathbf{x}) \ge \sum_{\mathbf{x}\in V_p\cap\mathscr{B}} 2^{-n}\,|\mathscr{B}| = 2^{-n}\,|\mathscr{B}|\,\big|\mathscr{B}\bigcap V_p\big|.$$

Thus, it follows

$$\big|\mathscr{B}\bigcap V_p\big| \le 2^{n+1}\Big(\frac{|\mathscr{B}|}{p} + p^{n/2}\Big),$$

which is the assertion of the lemma. □

An immediate result from the preceding Lemma is

Lemma 2.10. *Let $V_{p,\mathbb{Z}} = V_{p,\mathbb{Z}}(Q)$ be the set of integer solutions of the congruence* (2.16) *and let $\Delta_p = -1$. Then for any box $\mathscr{B}$ of type* (2.15),

$$\big|\mathscr{B}\bigcap V_{p,\mathbb{Z}}\big| \le 2^{n+1}\Big(\frac{|\mathscr{B}|}{p} + N_{\mathscr{B}}\;p^{n/2}\Big). \tag{2.57}$$

where $N_{\mathscr{B}}$ is given in (2.33).

Proof. We proceed just as in the proof of Lemma 2.7. Partition $\mathscr{B}$ into $N = N_{\mathscr{B}}$ smaller boxes B_i. This means

$$\mathscr{B} = \mathrm{B}_1 \bigcup \mathrm{B}_2 \bigcup \cdots \bigcup \mathrm{B}_N\,,$$

where each B_i has all of its edge lengths $\le p$. Apply Lemma 2.9 to each B_i, we thus obtain

$$\begin{aligned}\big|\mathscr{B}\bigcap V_{p,\mathbb{Z}}\big| &= \sum_{i=1}^{N}\big|\,\mathrm{B}_i\bigcap V_p\,\big| \\ &\overset{\text{(Lemma 2.9)}}{\uparrow}\le \sum_{i=1}^{N} 2^{n+1}\Big(\frac{|\mathrm{B}_i|}{p} + p^{n/2}\Big) \\ &= \frac{2^{n+1}}{p}\sum_{i=1}^{N}|\mathrm{B}_i| + N2^n\,p^{n/2}\end{aligned}$$

$$= 2^{n+1}\Big(\frac{|\mathscr{B}|}{p} + N\ p^{n/2}\Big),$$

finishing the proof of the lemma. □

By the fundamental identity (2.9) applied to $\alpha(\mathbf{x}) = \chi_{\mathscr{B}} * \chi_{\mathscr{B}}$ with $\Delta = -1$, and using the fact that $a(\mathbf{y}) \geq 0$ for all $\mathbf{y}$ we have

$$\sum_{\mathbf{x}\in V} \alpha(\mathbf{x}) \geq \underbrace{p^{-2}\sum_{\mathbf{x}} \alpha(\mathbf{x})}_{\text{Main Term}} - \underbrace{p^{n-1}\sum_{p|Q^*(\mathbf{y})} a(\mathbf{y})}_{E_1} - \underbrace{p^{(3n/2)-1}\sum_{\substack{p|Q^*(\mathbf{y}')\\ \mathbf{y}'(\mathrm{mod}\, p)}} a(p\mathbf{y}')}_{E_3}. \quad (2.58)$$

Next we are seeking to bound the error terms in (2.58). For the error term E_1 we have already seen in the case $\Delta = +1$ how this error term bounded. The same strategy will work in the case $\Delta = -1$, except we shall make use of the upper bound in (2.57) in Lemma 2.10 instead of the upper bound in (2.34) in Lemma 2.7. Indeed we find that

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

Thus, it follows that

$$E_1 \leq \underbrace{2^{4n+1} p^{n-2}\, |\mathscr{B}|}_{E_{1,1}} + \underbrace{\frac{2\cdot 4^n\, |\mathscr{B}|^2}{p^{n/2+1}} \prod_{i=1}^{n}\Big[\frac{4}{3} + \min\Big(\frac{2p}{m_i}, \frac{8p^2}{m_i^2}\Big)\Big]}_{E_{1,2}}. \quad (2.59)$$

Assume (as before) that

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

Then for $m_i \leq p$,

$$\frac{4}{3} + \min\Big(\frac{2p}{m_i}, 8\Big(\frac{p}{m_i}\Big)^2\Big) \leq \frac{4}{3} + \frac{2p}{m_i} \leq \frac{4p}{m_i},$$

and for $m_i > p$,

$$\frac{4}{3}+\min\Big(\frac{2p}{m_i},8\Big(\frac{p}{m_i}\Big)^2\Big)\le\frac{4}{3}+2\le\frac{10}{3}.$$

By taking account of these two inequalities, we have

$$\prod_{i=1}^{n}\Big[\frac{4}{3}+\min\Big(\frac{2p}{m_i},\frac{8p^2}{m_i^2}\Big)\Big]\le\prod_{i=1}^{l}\frac{4p}{m_i}\cdot\prod_{i=l+1}^{n}\frac{10}{3}=\frac{4^l p^l}{\prod_{i=1}^{l}m_i}\Big(\frac{10}{3}\Big)^{n-l}\le\frac{4^n p^l}{\prod_{i=1}^{l}m_i}. \tag{2.60}$$

Using (2.59) and (2.60), we infer that

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

To estimate the error term E_3, we just need to apply Lemma 2.8. It is easily seen that

$$E_3=p^{(3n/2)-1}\sum_{\mathbf{y}(\mathrm{mod}\,p)}a(p\mathbf{y})\le 2^{n-l}p^{l-(n/2)-1}|\mathscr{B}|\prod_{i=l+1}^{n}m_i. \tag{2.61}$$

However let us derive a good estimate for E_3, without using Lemma 2.8, hoping to get a better bound than the one in (2.61). Let $\mathbf{y}'$ runs through the set $\{y'\in\mathbb{Z}_p : Q^*(\mathbf{y}')\equiv 0(\mathrm{mod}\,p)\}$. Rewrite (2.35) to be for any $\mathbf{y}\in\mathbb{Z}_{p^2}^n$, with $|y_i|<p/2$,

$$a(\mathbf{y})=\prod_{i=1}^{n}a_i(y_i),$$

where

$$a_i(y_i)=\frac{1}{p^2}\frac{\sin^2\pi m_i y_i/p^2}{\sin^2\pi y_i/p^2},$$

and the term in the product is taken to be m_i if $y_i=0$ (as before). Then plainly

$$\big|a_i(y_i)\big|\le\frac{1}{p^2}\min\Big\{m_i^2,\frac{p^4}{4y_i^2}\Big\}=\min\Big\{\Big(\frac{m_i}{p}\Big)^2,\frac{p^2}{4y_i^2}\Big\}. \tag{2.62}$$

Replace each $\mathbf{y}$ by $p\mathbf{y}'$. Then, with $|y_i'|<p/2$, we have

$$\big|a(py_i')\big|\le\min\Big\{\Big(\frac{m_i}{p}\Big)^2,\frac{1}{4y_i'^2}\Big\}.$$

Thus

$$\sum_{y_i}^{p}\Big|a(p\mathbf{y})\Big| \le \sum_{\substack{\mathbf{y}\\ 1\le y_i\le p}} \prod_{i=1}^{n}\Big|a_i(py_i)\Big| = \prod_{i=1}^{n}\sum_{|y_i|<p/2}\big|a_i(py_i)\big|$$

$$\le \prod_{i=1}^{n}\sum_{|y_i|<p/2}\min\left\{\frac{m_i^2}{p^2},\frac{1}{4y_i^2}\right\}$$

$$\le \prod_{i=1}^{n}\left[\sum_{|y_i|\le p/2m_i}\frac{m_i^2}{p^2}+\sum_{|y_i|>p/2m_i}\frac{1}{4y_i^2}\right]$$

(Using the fact: $\sum_{n=1}^{\infty}\frac{1}{n^2}=\frac{\pi^2}{6}$ and continuing),

$$\le \prod_{i=1}^{n}\left[\left(\frac{p}{m_i}+1\right)\frac{m_i^2}{p^2}+\frac{1}{4}2\frac{\pi^2}{6}\right]=\prod_{i=1}^{n}\left(\frac{m_i}{p}+\frac{m_i^2}{p^2}+1\right).$$

Suppose that

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

Then obviously

$$\sum_{\mathbf{y}}\Big|a(p\mathbf{y})\Big| \le \prod_{i=1}^{l}3\prod_{i=l+1}^{n}3\left(\frac{m_i^2}{p^2}\right)=3^n\prod_{i=l+1}^{n}\left(\frac{m_i^2}{p^2}\right).$$

Hence it follows

$$E_3 \le 3^n\,p^{(3n/2)-1}\prod_{i=l+1}^{n}\left(\frac{m_i^2}{p^2}\right). \tag{2.63}$$

A special case, when $l=0$ in (2.63), we have

$$E_3 \le 3^n\,p^{(3n/2)-1}\,\frac{|\mathscr{B}|^2}{p^{2n}}=3^n\,p^{-[(n/2)+1]}\,|\mathscr{B}|^2.$$

Comparing these two estimates in (2.61) and (2.63), we conclude that the estimate in (2.61) still is better.

Hence, we summarize in

Theorem 2.4. *Suppose that $n\ge 4$ is even, and that $\Delta_p(Q)=-1$. Then for any box $\mathscr{B}$ centered at the origin,*

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

where

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

As before, in order to obtain a positive sum we seek conditions such that each error term is less than ¼ of the main term.

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

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

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

Thus we obtain,

Theorem 2.5. *Suppose that* $n \geq 4$ *is even, and that* $\Delta_p(Q) = -1$. *If* $|\mathscr{B}| \geq 2^{4n+3} p^n$ *and* $\prod_{i=1}^{l}(p/m_i) \leq 2^{-4n-3} p^{(n/2)-1}$ (*with L.H.S* $= 1$ *if* $l = 0$), *then*

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

In particular

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

As a consequence of Theorem 2.5, we have the following analogue of Corollary 2.2 for primitive solutions.

Corollary 2.4. *Under the hypotheses of Theorem* 2.5, $\mathscr{B} + \mathscr{B}$ *contains a primitive solution of* (2.1).

Proof. Everything almost works the same as in Corollary 2.1. We must prove that

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

First we have with the help of Lemma 2.8,

$$\sum_{\substack{\mathbf{x}\in V \\ p|\mathbf{x}}} \alpha(\mathbf{x}) = \sum_{\substack{p|x_i, \\ 1\leq i\leq n}} \alpha(\mathbf{x}) = p^n \sum_{y_i=1}^{p} a(p\mathbf{y}) \leq 2^{n-l} p^{l-n} |\mathscr{B}| \prod_{i=l+1}^{n} m_i$$

$$= \frac{1}{2^l} \cdot \frac{2^n |\mathscr{B}|}{p^{n-l}} \prod_{i=l+1}^{n} m_i \leq \frac{1}{2^l} \cdot \frac{|\mathscr{B}|^2}{4p^2}. \tag{2.64}$$

Here the last inequality in (2.64) is true by our hypothesis (Theorem 2.5) that

$$\prod_{i=1}^{l} \frac{p}{m_i} \leq 2^{-4n-2} p^{(n/2)-1}. \tag{2.65}$$

Let us pause the proof for moment and verify that this hypothesis gives us the last inequality. So we may assume (2.65). Then

$$\begin{aligned} \prod_{i=1}^{l} \frac{p}{m_i} \leq \frac{p^{n/2}}{2^{4n+2}} \;&\Rightarrow\; 2^{4n+2} p^{l-(n/2)} \leq \prod_{i=1}^{l} m_i \\ &\Rightarrow\quad 2^{4n} p^{l-(n/2)-2} \prod_{i=l+1}^{n} m_i \leq \frac{|\mathscr{B}|}{4p^2} \\ &\Rightarrow\quad 2^{n} p^{l-n} \prod_{i=l+1}^{n} m_i \leq \frac{|\mathscr{B}|}{4p^2}. \end{aligned}$$

We resume our proof. Since we now have

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

and Theorem 2.5 yields

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

we thus obtain

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

which give us the desired conclusion. □

We now turn our attention to the following special cases.

Corollary 2.5. *Let $\mathscr{B}$ be a cube centered at the origin with all $m_i = B$ $B > 2^{4+(3/n)} p$ and $p \geq 2^{(8n+6)/(n-2)}$ and $\Delta_p = -1$. Then $\mathscr{B} + \mathscr{B}$ contains a primitive solution of* (2.1).

Proof. This follows as in the proof of the Corollary 2.2 of the preceding section. Just by assuming that $B > 2^{4+(3/n)} p$, and $p \geq 2^{(8n+4)/(n-2)}$, we have then $l = 0$ and the hypotheses of Corollary 2.4 are satisfied. □

Corollary 2.6. *Let* $\mathscr{B}$ *be a rectangular box centered at the origin with*

$$m_1 = \cdots = m_l = 1, \;\; m_{l+1} = \cdots = m_n \geq 2^{(4n+2)/(n-l)} p^{n/(n-l)},$$

for some $l \leq (n/2) - 2$ *and*

$$p \geq 2^{4(2n+1)/(n-2l)}.$$

Then $\mathscr{B} + \mathscr{B}$ *contains a primitive solution* (2.1).

Proof. Assume that the conditions of Corollary 2.6 hold. Then

$$\prod_{i=1}^{l} (p/m_i) \leq 2^{-4n-2} p^{(n/2)},$$

is implied by

$$p \geq 2^{4(2n+1)/(n-2l)}.$$

Indeed, by hypothesis $\prod_{i=1}^{l} (p/m_i) = p^l$, and

$$p^l \leq 2^{-4n-2} p^{n/2},$$

if and only if

$$p \geq 2^{2(4n+2)/(n-2l)}.$$

We also have,

$$|\mathscr{B}| \geq 2^{(4n+2)(n-l)/(n-l)} p^{n(n-l)/(n-l)} = 2^{(4n+2)} p^n.$$

Hence Corollary 2.4 applies. □

We conclude this chapter with

Proof of Theorem 2.1. This theorem follows immediately from Corollary 2.2. (gives us (2.3)) and Corollary 2.5 (gives us (2.4)) upon setting $n = 4$. □

Chapter 3

Small Zeros of Quadratic Forms Modulo p^3

§3.1. Introduction.

Let $Q(\mathbf{x}) = Q(x_1, x_2, ..., x_n) = \sum_{1 \le i \le j \le n} a_{ij} x_i x_j$ be a quadratic form with integer coefficients and p be an odd prime. Set $\|\mathbf{x}\| = \max |x_i|$. Let $V_{p^3} = V_{p^3}(Q)$ be the set of zeros of Q contained in $\mathbb{Z}_{p^3}^n$. When n is even we let

$$\Delta_p(Q) = \begin{cases} \left((-1)^{n/2} \det A_Q \,/\, p \right) & \text{if} \quad p \nmid \det A_Q, \\ 0 & \text{if} \quad p \mid \det A_Q, \end{cases}$$

where $(\bullet / p)$ denotes the Legendre-Jacobi symbol and A_Q is the $n \times n$ defining matrix for $Q(\mathbf{x})$. For $\mathbf{y} \in \mathbb{Z}_{p^3}^n$ set

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

where $e_{p^3}(x) = e^{2\pi i x / p^3}$.

We shall devote this chapter to generalize the method for $(\mathrm{mod}\, p^2)$ to $(\mathrm{mod}\, p^3)$. Our goal is to find a primitive solution of the congruence

$$Q(\mathbf{x}) \equiv 0 \pmod{p^3}, \tag{3.1}$$

with $\mathbf{x} \in \mathscr{B}$, where $\mathscr{B}$ is any box with $|\mathscr{B}|$ sufficiently large. In particular we wish to obtain the existence of a nontrivial solution of

(3.1) with $\|\mathbf{x}\|$ as small as possible. To this end we shall build lemmas, theorems and corollaries analogous to those in Chapter 2.

In Chapter 4, we shall prove the following fundamental identity (Theorem 4.2): For any complex valued function $\alpha(\mathbf{x})$ defined on $\mathbb{Z}_{p^m}^n$ with finite Fourier expansion $\alpha(\mathbf{x})=\sum_{\mathbf{y}} a(\mathbf{y})\, e_{p^m}(\mathbf{x}\cdot\mathbf{y})$, where $a(\mathbf{y})= p^{-mn}\times \sum_{\mathbf{x}}\alpha(\mathbf{x})e_{p^m}(-\mathbf{x}\cdot\mathbf{y})$ we have

$$\sum_{\mathbf{x}\in V_{p^m}} \alpha(\mathbf{x}) = p^{-m} \sum_{\mathbf{x}\,(\mathrm{mod}\, p^m)} \alpha(\mathbf{x}) + p^{mn/2}\sum_{j=0}^{m-1} p^{jn/2}\delta_j\Bigg(p^{-j} \sum_{\substack{y_i'=1 \\ p^{m-j}\mid Q^*(\mathbf{y}')}}^{p^{m-j}} a(p^j\mathbf{y}') - p^{-j-1} \sum_{\substack{y_i'=1 \\ p^{m-j-1}\mid Q^*(\mathbf{y}')}}^{p^{m-j}} a(p^j\mathbf{y}')\Bigg).$$

where δ_j is defined:

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

Thus when $m=3$, we have

$$\begin{aligned}\sum_{\mathbf{x}\in V_{p^3}} \alpha(\mathbf{x}) = p^{-3}\sum_{\mathbf{x}} \alpha(\mathbf{x}) + p^{3n/2}\Bigg\{ &\Delta\Bigg(\sum_{\substack{y_i'=1 \\ p^3\mid Q^*(\mathbf{y}')}}^{p^3} a(\mathbf{y}') - p^{-1} \sum_{\substack{y_i'=1 \\ p^2\mid Q^*(\mathbf{y}')}}^{p^3} a(\mathbf{y}')\Bigg) \\ &+ p^{n/2}\Bigg(p^{-1} \sum_{\substack{y_i'=1 \\ p^2\mid Q^*(\mathbf{y}')}}^{p^2} a(p\mathbf{y}') - p^{-2} \sum_{\substack{y_i'=1 \\ p\mid Q^*(\mathbf{y}')}}^{p^2} a(p\mathbf{y}')\Bigg) \\ &+ \Delta p^n\Bigg(p^{-2} \sum_{\substack{y_i'=1 \\ p\mid Q^*(\mathbf{y}')}}^{p} a(p^2\mathbf{y}') - p^{-3}\sum_{y_i'=1}^{p} a(p^2\mathbf{y}')\Bigg)\Bigg\} \quad (3.2)\end{aligned}$$

The first term on the right-hand side is the main term, and the remaining terms are the error terms. In order to estimate the error terms we first need to obtain good upper bounds for $\left|V_{p^2} \cap \mathscr{B}\right|$.

§3.2. Estimating $\left|V_{p^2} \cap \mathscr{B}\right|$.

In this section we try to find and prove the analogue of Lemma 2.5, Lemma 2.6 and Lemma 2.7 of Chapter 2, for an arbitrary box.

Let

$$\mathscr{B} = \Big\{ \mathbf{x} \in \mathbb{Z}^n \,\Big|\, a_i \le x_i < a_i + m_i, 1 \le i \le n \Big\}. \tag{3.3}$$

where $a_i, m_i \in \mathbb{Z}, 1 \le m_i \le p^2, 1 \le i \le n$. Then $|\mathscr{B}| = \prod_{i=1}^n m_i$, the cardinality of $\mathscr{B}$. View the box $\mathscr{B}$ in (3.3) as a subset of $\mathbb{Z}_{p^2}^n$ and let $\chi_{\mathscr{B}}$ be it characteristic function with Fourier expansion

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

Consider the congruence

$$Q(\mathbf{x}) \equiv 0 \pmod{p^2}, \tag{3.4}$$

where $Q(\mathbf{x})$ is a quadratic form. Later we need to develop a good bound for the error term $\sum_{p^2 | Q^*(\mathbf{y})} a(\mathbf{y})$ and to do this we need to estimate $\left| V_{p^2} \bigcap \mathscr{B} \right|$ first.

Lemma 3.1. *Let p be an odd prime, $V_{p^2} = V_{p^2}(Q)$ be the set of zeros of (3.4) in $\mathbb{Z}_{p^2}^n$, and $\mathscr{B}$ be a box as given in (3.3) centered at the origin with all $m_i \le p^2$. If $\Delta_p = \pm 1$, then*

$$\left| \mathscr{B} \bigcap V_{p^2} \right| \le \vartheta_n \left(\frac{|\mathscr{B}|}{p^2} + p^n \right). \tag{3.5}$$

where

$$\vartheta_n = \begin{cases} 2^n \left(1 + \dfrac{2^{(n/2)+1}}{p} \right), & \Delta = -1, \\ 2^n \left(1 + 2^{(n/2)+1} \right), & \Delta = +1. \end{cases} \tag{3.6}$$

Proof. The idea of the proof is similar to the ideas used to prove Lemma 2.5 of Chapter 2. We begin by writing the fundamental identity (mod p^2):

$$\begin{aligned} \sum_{\mathbf{x} \in V_{p^2}} \alpha(\mathbf{x}) = p^{-2} \sum_{\mathbf{x}} \alpha(\mathbf{x}) + p^n \sum_{\substack{y_i = 1 \\ p^2 | Q^*(\mathbf{y})}}^{p^2} a(\mathbf{y}) - p^{n-1} \sum_{\substack{y_i = 1 \\ p | Q^*(\mathbf{y})}}^{p^2} a(\mathbf{y}) \\ - \Delta p^{(3n/2)-2} \sum_{y_i' = 1}^{p} a(p\mathbf{y}') + \Delta p^{(3n/2)-1} \sum_{\substack{y_i' = 1 \\ p | Q^*(\mathbf{y}')}}^{p} a(p\mathbf{y}'). \end{aligned} \tag{3.7}$$

Set $\alpha = \chi_{\mathscr{B}} * \chi_{\mathscr{B}} = \sum_{\mathbf{y}} a(\mathbf{y}) e_{p^2}(\mathbf{x}\cdot\mathbf{y})$. Then the Fourier coefficients of $\alpha(\mathbf{x})$

are given by $a(\mathbf{y}) = p^{2n} a_{\mathscr{B}}^2(\mathbf{y})$ and since $\mathscr{B}$ is centered at the origin, these are positive real numbers. By Parseval's identity we have

$$\sum_{\mathbf{y}} \left|a(\mathbf{y})\right| = p^{2n} \sum_{\mathbf{y}} \left|a_{\mathscr{B}}(\mathbf{y})\right|^2 = \sum_{\mathbf{y}} \left|\chi_{\mathscr{B}}(\mathbf{y})\right|^2 = |\mathscr{B}|. \tag{3.8}$$

Thus, it follows from (3.8),

$$p^n \sum_{\substack{y_i=1 \\ p^2 | Q^*(\mathbf{y})}}^{p^2} a(\mathbf{y}) \le p^n \sum_{\mathbf{y}} \left|a(\mathbf{y})\right| \le p^n \, |\mathscr{B}|. \tag{3.9}$$

Notice that the main term in (3.7) is

$$p^{-2} \sum_{\mathbf{x}} \alpha(\mathbf{x}) = p^{-2} \sum_{\mathbf{x}} \chi_{\mathscr{B}} * \chi_{\mathscr{B}}(\mathbf{x}) = \frac{|\mathscr{B}|^2}{p^2}. \tag{3.10}$$

By Lemma 2.8 of Chapter 2, we have

$$p^{(3n/2)-2} \sum_{y_i'=1}^{p} a(p\mathbf{y}') \le 2^{n-l} p^{l-(n/2)-2} \, |\mathscr{B}| \prod_{i=l+1}^{n} m_i \,, \tag{3.11}$$

and

$$p^{(3n/2)-1} \sum_{\substack{y_i'=1 \\ p | Q^*(\mathbf{y}')}}^{p} a(p\mathbf{y}') \le p^{(3n/2)-1} \sum_{\mathbf{y}'} a(p\mathbf{y}') \le 2^{n-l} p^{l-(n/2)-1} \, |\mathscr{B}| \prod_{i=l+1}^{n} m_i, \tag{3.12}$$

where as defined in chapter 2, l is defined by

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

The case $\Delta_p(Q) = -1$:

Now going back to (3.7), if $\Delta = -1$, we have

$$\sum_{\mathbf{x} \in V_{p^2}} \alpha(\mathbf{x}) \le p^{-2} \sum_{\mathbf{x}} \alpha(\mathbf{x}) + p^n \sum_{\substack{y_i=1 \\ p^2 | Q^*(\mathbf{y})}}^{p^2} a(\mathbf{y}) + p^{(3n/2)-2} \sum_{y_i'=1}^{p} a(p\mathbf{y}') \tag{3.13}$$

Then by the equalities in (3.9), (3.10), and (3.11), we obtain

$$\sum_{\mathbf{x} \in V_{p^2}} \alpha(\mathbf{x}) \le \underbrace{\frac{|\mathscr{B}|^2}{p^2}}_{①} + \underbrace{p^n \, |\mathscr{B}|}_{②} + \underbrace{2^{n-l} p^{l-(n/2)-2} \, |\mathscr{B}| \prod_{i=l+1}^{n} m_i}_{③}. \tag{3.14}$$

We next determine which of the terms ①, ②, and ③ in (3.14) is the dominant term. We consider two cases:

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

$$\frac{③}{①} = \frac{2^{n-l}\, p^{l-(n/2)-2}\, |\mathscr{B}| \prod_{i=l+1}^{n} m_i}{|\mathscr{B}|^2 / p^2} = \frac{1}{|\mathscr{B}|}\, p^{l-(n/2)} 2^{n-l} \prod_{i=l+1}^{n} m_i = \frac{p^{l-(n/2)} 2^{n-l}}{\prod_{i=1}^{l} m_i}$$
$$\leq 2^{n-l}\, p^{l-(n/2)} = 2^n \left(\frac{p}{2}\right)^l p^{-n/2} \leq 2^n \left(\frac{p}{2}\right)^{(n/2)-1} p^{-n/2} \leq 2^{(n/2)+1} \cdot \frac{1}{p},$$

which implies that

$$③ \ \leq \frac{2^{(n/2)+1}}{p} \ ① \quad \text{or} \quad 2^n\, p^{l-(n/2)-2}\, |\mathscr{B}| \prod_{i=l+1}^{n} m_i \leq \frac{2^{(n/2)+1}}{p} \frac{|\mathscr{B}|^2}{p^2}.$$

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

$$\frac{③}{②} = \frac{2^{n-l}\, p^{l-(n/2)-2}\, |\mathscr{B}| \prod_{i=l+1}^{n} m_i}{p^n\, |\mathscr{B}|} = 2^{n-l}\, p^{l-(3n/2)-2} \prod_{i=l+1}^{n} m_i$$
$$\leq 2^n\, p^{l-(3n/2)-2} p^{2(n-l)} = 2^{n-l}\, p^{n/2-2-l} \leq \frac{2^{n/2}}{p^2}$$

which leads to

$$③ \leq \frac{2^{n/2}}{p^2} ② \quad \text{or} \quad 2^n\, p^{l-(n/2)-2}\, |\mathscr{B}| \prod_{i=l+1}^{n} m_i \leq \frac{2^{n/2}}{p^2}\, p^n\, |\mathscr{B}|.$$

So for any l, always we have

$$③ \ \leq \left(\frac{2^{(n/2)+1}}{p} ① + \frac{2^{n/2}}{p^2} ②\right),$$

or,

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

Returning to (3.14), we now can write

$$\sum_{\mathbf{x} \in V_{p^2}} \alpha(\mathbf{x}) \leq ① + ② + ③$$
$$\leq ① + ② + \frac{2^{(n/2)+1}}{p} ① + \frac{2^{n/2}}{p^2} ②$$
$$= \left(1 + \frac{2^{(n/2)+1}}{p}\right)① + \left(1 + \frac{2^{n/2}}{p^2}\right)②$$
$$\leq \vartheta_n' \left(\frac{|\mathscr{B}|^2}{p^2} + p^n\, |\mathscr{B}|\right), \tag{3.15}$$

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

$$\sum_{\mathbf{x} \in V_{p^2}} \alpha(\mathbf{x}) \geq \frac{1}{2^n} |\mathscr{B}| \left| V_{p^2} \cap \mathscr{B} \right|. \tag{3.16}$$

To ensure that the above inequality (3.16) is true see the proof of

Lemma 2.5 of Chapter 2. Hence it follows by combining (3.15) and (3.16) that

$$\Big|\mathscr{B} \bigcap V_{p^2}\Big| \le 2^n \vartheta_n' \Big(\frac{|\mathscr{B}|}{p^2} + p^n\Big). \tag{3.17}$$

The case $\Delta_p(Q) = +1$**:**

If $\Delta_p = +1$, again by (3.7), we have

$$\begin{aligned}\sum_{\mathbf{x}\in V_{p^2}} \alpha(\mathbf{x}) &\le p^{-2}\sum_{\mathbf{x}} \alpha(\mathbf{x}) + p^n \sum_{\mathbf{y}} \big|a(\mathbf{y})\big| + p^{(3n/2)-1} \sum_{\mathbf{y} (\mathrm{mod}\, p)} a(p\mathbf{y}) \\ &\underset{\substack{\uparrow \\ (3.10),(3.9)\&(3.12)}}{\le} \underbrace{\frac{|\mathscr{B}|^2}{p^2}}_{①} + \underbrace{p^n\,|\mathscr{B}|}_{②} + \underbrace{2^{n-l}\, p^{l-(n/2)-1}\,|\mathscr{B}| \prod_{i=l+1}^{n} m_i}_{④}. \end{aligned} \tag{3.18}$$

We do a similar investigation (as before) to determine which of the terms ①, ②, and ④ of the inequality (3.18) is the dominant term. In case (i) we find $④/① \le 2^{(n/2)+1}$, which means that $④ \le 2^{(n/2)+1}\,①$. And in case (ii) we find $④/② \le 2^{n/2}/p$, which gives us that $④ \le 2^{n/2}/p\;②$. Hence for any l, we always have

$$④ \;\le \Big(2^{(n/2)+1}\;① + \frac{2^{n/2}}{p}\;②\Big),$$

or,

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

Now in looking at (3.18), one easily deduces

$$\begin{aligned}\sum_{\mathbf{x}\in V_{p^2}} \alpha(\mathbf{x}) &\le (1 + 2^{(n/2)+1})\,\frac{|\mathscr{B}|^2}{p^2} + \Big(1 + \frac{2^{n/2}}{p}\Big)p^n\,|\mathscr{B}| \\ &\le \vartheta_n'' \Big(\frac{|\mathscr{B}|^2}{p^2} + p^n\,|\mathscr{B}|\Big),\end{aligned}$$

where $\vartheta_n'' = 1 + 2^{(n/2)+1}$. Thus by (3.16),

$$\Big|\mathscr{B} \bigcap V_{p^2}\Big| \le \frac{2^n}{|\mathscr{B}|} \sum_{\mathbf{x}\in V_{p^2}} \alpha(\mathbf{x}) = \vartheta_n'' 2^n \Big(\frac{|\mathscr{B}|}{p^2} + p^n\Big).$$

Lastly letting $\vartheta_n = 2^n \vartheta_n'$ if $\Delta = -1$ and $\vartheta_n = \vartheta_n''$ if $\Delta = +1$ we get from (3.15) and (3.19) that for $\Delta = \pm 1$, one always has

$$\Big|\mathscr{B} \bigcap V_{p^2}\Big| \le \vartheta_n \Big(\frac{|\mathscr{B}|}{p^2} + p^n\Big).$$

This achieves the proof of the lemma. □

For our purpose we have to drop the hypothesis "centered at the origin" in Lemma 3.1.

Lemma 3.2. *Let p be an odd prime, $V_{p^2} = V_{p^2}(Q)$ be the set of zeros of* (3.4) *in $\mathbb{Z}_{p^2}^n$, and $\mathscr{B}$ be any box as given in* (3.3) *with all $m_i \le p^2$. If $\Delta_p = \pm 1$, then*

$$\left|\mathscr{B} \bigcap V_{p^2}\right| \le \gamma_n\left(\frac{|\mathscr{B}|}{p^2} + p^n\right). \tag{3.19}$$

where

$$\gamma_n = 2^n(1+6^n)\ . \tag{3.20}$$

***Proof of Lemma* 3.2.** We proceed as in the proof of Lemma 2.6. The fundamental identity $(\bmod p^2)$ is

$$\begin{aligned}\sum_{\mathbf{x}\in V_{p^2}} \alpha(\mathbf{x}) = p^{-2}\sum_{\mathbf{x}} \alpha(\mathbf{x}) + \underbrace{p^n \sum_{\substack{y_i=1\\ p^2\mid Q^*(\mathbf{y})}}^{p^2} a(\mathbf{y})}_{E_0} - \underbrace{p^{n-1} \sum_{\substack{y_i=1\\ p\mid Q^*(\mathbf{y})}}^{p^2} a(\mathbf{y})}_{E_1} \\ \underbrace{-\Delta p^{(3n/2)-2} \sum_{y_i'=1}^{p} a(p\mathbf{y}')}_{E_2} + \underbrace{\Delta p^{(3n/2)-1} \sum_{\substack{y_i'=1\\ p\mid Q^*(\mathbf{y}')}}^{p} a(p\mathbf{y}')}_{E_3}.\end{aligned} \tag{3.21}$$

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

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

Then

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

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

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

Again, by using the Cauchy-Schwartz inequality and Parseval's identity, (1.10) of Chapter 1, we get

$$\sum_{\mathbf{y}} \left|a(\mathbf{y})\right| \le |\mathscr{B}|.$$

Then

$$\left|E_0 - E_1\right| = \left| p^n \sum_{\substack{y_i=1 \\ p^2 \mid Q^*(\mathbf{y})}}^{p^2} a(\mathbf{y}) - p^{n-1} \sum_{\substack{y_i=1 \\ p \mid Q^*(\mathbf{y})}}^{p^2} a(\mathbf{y}) \right| = \left| \sum_{y_i=1}^{p^2} \psi(\mathbf{y}) a(\mathbf{y}) \right|, \quad (3.22)$$

where

$$\psi(\mathbf{y}) = \begin{cases} p^n - p^{n-1}, & p^2 \left| Q^*(\mathbf{y}), \right. \\ -p^{n-1}, & p \left\| Q^*(\mathbf{y}). \right. \end{cases}$$

Then continuing from (3.22),

$$\left|E_0 - E_1\right| \le (p^n - p^{n-1}) \sum_{\mathbf{y}} \left|a(\mathbf{y})\right| \le (p^n - p^{n-1}) |\mathscr{B}|.$$

Also,

$$\left|E_2 - E_3\right| = \left| -\Delta p^{(3n/2)-2} \sum_{y_i'=1}^{p} a(p\mathbf{y}') + \Delta p^{(3n/2)-1} \sum_{\substack{y_i'=1 \\ p \mid Q^*(\mathbf{y}')}}^{p} a(p\mathbf{y}') \right| \le \left| \sum_{y_i'=1}^{p} \theta(\mathbf{y}')\, a(p\mathbf{y}') \right|, \quad (3.23)$$

where

$$\theta(\mathbf{y}) = \begin{cases} p^{(3n/2)-1} - p^{(3n/2)-2}, & p \left| Q^*(\mathbf{y}), \right. \\ p^{(3n/2)-2}, & p \nmid Q^*(\mathbf{y}). \end{cases}$$

Then continuing from (3.23),

$$\left|E_2 - E_3\right| \le (p^{3n/2-1} - p^{3n/2-2}) \sum_{y_i'=1}^{p} \left|a(p\mathbf{y}')\right|. \quad (3.24)$$

To complete the proof of Lemma 3.2, we need the following Lemma,

Lemma 3.3.

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

Proof. We begin by establishing the inequality

$$\sum_{|y_i|>p/2m_i} \frac{1}{4y_i^2} \le \begin{cases} 4\frac{m_i}{p} & \text{if} \quad m_i \le p/2, \\ 1 & \text{if} \quad m_i > p/2. \end{cases} \quad (3.25)$$

We split the proof into two cases.

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

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

Then

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

So

$$\sum_{|y_i| > p/2m_i} \frac{1}{4y_i^2} \leq 4\frac{m_i}{p}.$$

***Case* (II):** If $\frac{p}{2m_i} < 1$, then by (2.62) of Chapter 2 (see page 50),

$$\sum_{|y_i| > p/2m_i} \frac{1}{4y_i^2} \leq \frac{2}{4}\sum_{y=1}^{\infty} \frac{1}{y^2} \leq \frac{\pi^2}{3 \cdot 4} = \frac{\pi^2}{12} \leq 1.$$

By ***case* I** and ***case* II**, (3.25) follows.

We return to the proof of the lemma. Say $a(\mathbf{y}) = \prod_{i=1}^{n} a_i(y_i)$. Then by the Fourier coefficients $a(\mathbf{y}) = p^{2n} a_{\mathscr{B}}(\mathbf{y})\, a_{\mathscr{B}'}(\mathbf{y})$,

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

and so

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

We consider four cases:

***Case* (i):** If $m_i \leq \frac{p}{2}$,then

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

***Case* (ii):** If $m_i > \frac{p}{2}$,then

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

***Case* (iii):** If $\frac{p}{2}<m_i<p,$ then

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

***Case* (iv):** If $m_i>p$,then

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

completing the proof of lemma 3.3. □

***Continue the proof of Lemma* 3.2.** Suppose

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

By Lemma 3.3,

$$\sum_{|\mathbf{y}|<p/2}\left|a_i(p\mathbf{y})\right|=\prod_{i=1}^{n}\sum_{|y_i|<p/2}\left|a_i(py_i)\right|=\prod_{m_i\le p}6\frac{m_i}{p}\prod_{m_i>p}3\frac{m_i^2}{p^2}$$
$$\le 3^n2^l\frac{|\mathscr{B}|}{p^n}\prod_{m_i>p}\frac{m_i}{p}=3^n2^l\frac{|\mathscr{B}|}{p^n}\frac{\prod_{m_i>p}m_i}{p^{n-l}}. \tag{3.26}$$

Using (3.26), then continuing from (3.24)

$$\left|E_2-E_3\right|\le p^{(3n/2)-2}(p-1)\cdot 3^n2^lp^{l-2n}\left|\mathscr{B}\right|\prod_{i=l+1}^{n}m_i\,.$$

Thus for $\Delta=\pm1,$ the fundamental identity gives

$$\sum_{\mathbf{x}\in V_{p^2}}\alpha(\mathbf{x})\le\frac{|\mathscr{B}|^2}{p^2}+\left|E_0-E_1\right|+\left|E_2-E_3\right|$$
$$\le\frac{|\mathscr{B}|}{p^2}+(p^n-p^{n-1})|\mathscr{B}|+p^{(3n/2)-2}(p-1)\cdot 3^n2^lp^{l-2n}\left|\mathscr{B}\right|\prod_{i=l+1}^{n}m_i$$
$$\le\underbrace{\frac{|\mathscr{B}|^2}{p^2}}_{①}+\underbrace{p^n\,|\mathscr{B}|}_{②}+\underbrace{3^n2^lp^{l-(n/2)-1}\left|\mathscr{B}\right|\prod_{i=l+1}^{n}m_i}_{❸}\,. \tag{3.27}$$

The task now is determining which of the terms ①, ②, and ❸ in (3.27) is the dominant term. We consider two cases:

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

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

This leads to

$$❸ \ \le 3^n 2^l \ \ ①.$$

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

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

This gives that

$$❸ \le \frac{3^n 2^l}{p}\ ②.$$

So for any l, we always have

$$❸ \ \le \left(3^n 2^l\ ① + \frac{3^n 2^l}{p}\ ②\right).$$

Returning to (3.27), we now can write

$$\sum_{\mathbf{x} \in V_{p^2}} \alpha(\mathbf{x}) \le ① + ② + ❸$$
$$\le ① + ② + 3^n 2^l\ ① + \frac{3^n 2^l}{p}\ ②$$
$$= \left(1 + 3^n 2^l\right) ① + \left(1 + \frac{3^n 2^l}{p}\right) ②$$
$$\le \gamma_n' \left(\frac{|\mathscr{B}|^2}{p^2} + p^n\, |\mathscr{B}|\right), \tag{3.28}$$

where $\gamma_n' = 1 + 3^n 2^l$. On the other hand, as in the proof of Lemma 2.6 we know that

$$\sum_{\mathbf{x} \in V_{p^2}} \alpha(\mathbf{x}) \ge \frac{1}{2^n} |\mathscr{B}| \left|V_{p^2} \bigcap \mathscr{B}\right|. \tag{3.29}$$

Hence it follows by combining (3.28) and (3.29) that

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

where $\gamma_n = 2^n (1 + 6^n)$. Lemma 3.2 is proved. □

§3.3. Bounds on the error terms in the Fundamental identity (mod p^3). The case of $\Delta = +1$.

Putting $\Delta = +1$ in (3.2), we obtain

$$\begin{aligned}\sum_{\mathbf{x}\in V_{p^3}} \alpha(\mathbf{x}) &= p^{-3}\sum_{\mathbf{x}} \alpha(\mathbf{x}) \\ &+ \underbrace{p^{3n/2}\sum_{\substack{y_i'=1\\ p^3|Q^*(\mathbf{y}')}}^{p^3} a(\mathbf{y}')}_{Er_1} + \underbrace{p^{2n-1}\sum_{\substack{y_i'=1\\ p^2|Q^*(\mathbf{y}')}}^{p^2} a(p\mathbf{y}')}_{Er_2} + \underbrace{p^{5n/2-2}\sum_{\substack{y_i'=1\\ p|Q^*(\mathbf{y}')}}^{p} a(p^2\mathbf{y}')}_{Er_3} \\ &- \underbrace{p^{(3n/2)-1}\sum_{\substack{y_i'=1\\ p^2|Q^*(\mathbf{y}')}}^{p^3} a(\mathbf{y}')}_{Er_4} - \underbrace{p^{2n-2}\sum_{\substack{y_i'=1\\ p|Q^*(\mathbf{y}')}}^{p^2} a(p\mathbf{y}')}_{Er_5} - \underbrace{p^{5n/2-3}\sum_{y_i'=1}^{p} a(p^2\mathbf{y}')}_{Er_6}\end{aligned} \tag{3.30}$$

Throughout the section and next, for convenience, Er_i or Er_{ij}, $i, j \in \{1,2,3,4,5,6\}$ will indicate an error term or a value bounding that error term.

We apply the identity in (3.30) to the function $\alpha(x) = \chi_{\mathscr{B}} * \chi_{\mathscr{B}}$ where $\mathscr{B}$ is a box centered at the origin, given by

$$\mathscr{B} = \Big\{\mathbf{x} \in \mathbb{Z}^n \,\Big|\, a_i \le x_i < a_i + m_i, 1 \le i \le n\Big\}. \tag{3.31}$$

where $a_i, m_i \in \mathbb{Z}, 1 \le m_i \le p^3, 1 \le i \le n$.

For later reference, we construct a series of lemmas analagous to those of Chapter 2.

Lemma 3.4. Let $\mathscr{B}$ be any box of type (3.3) and $\alpha(\mathbf{x}) = \chi_{\mathscr{B}} * \chi_{\mathscr{B}}(\mathbf{x})$. Then we have

$$\sum_{y_i=1}^{p^2} a(p\mathbf{y}) \le \frac{|\mathscr{B}|}{p^n} \prod_{m_i \ge p^2} \frac{2m_i}{p^2}.$$

Proof. First,

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

$$= \frac{1}{p^{3n}} \sum_{\substack{x_i=1 \\ \mathbf{x}\equiv 0 \,(\mathrm{mod}\, p^2)}}^{p^2} \alpha(\mathbf{x}) p^{2n}$$

$$= \frac{1}{p^n} \sum_{\mathbf{x}\equiv 0 \,(\mathrm{mod}\, p^2)} \alpha(\mathbf{x})$$

$$= \frac{1}{p^n} \sum_{\substack{\mathbf{u}\in\mathscr{B} \\ \mathbf{u}+\mathbf{v}\equiv 0 \,(\mathrm{mod}\, p^2)}} \sum_{\mathbf{v}\in\mathscr{B}} 1 \tag{3.32}$$

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

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

with $\mathbf{u}, \mathbf{v} \in \mathscr{B}$. In fact for each choice of $\mathbf{v}$, there are at most $\prod_{i=1}^{n}([m_i / p^2]+1)$ choices 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 (3.32),

$$\sum_{y_i=1}^{p^2} a(p\mathbf{y}) \le \frac{1}{p^n} \prod_{i=1}^{n} m_i \left(\left[\frac{m_i}{p^2} \right] + 1 \right). \tag{3.33}$$

We split the product in (3.33) to get

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

Then by the help of this inequality we obtain

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

proving the lemma. □

Lemma 3.5. Let $\mathscr{B}$ be any box of type (3.3) and $\alpha(\mathbf{x}) = \chi_{\mathscr{B}} * \chi_{\mathscr{B}}(\mathbf{x})$. Then we have

$$\sum_{y_i=1}^{p} a(p^2\mathbf{y}) \le \frac{|\mathscr{B}|}{p^{2n}} \prod_{m_i \ge p} \frac{2m_i}{p}.$$

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

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

$$= \sum_{x_i=1}^{p^3} \frac{1}{p^{3n}} \alpha(\mathbf{x}) \sum_{y_i=1}^{p} e_p(-\mathbf{x} \cdot \mathbf{y})$$

$$
\begin{aligned}
&= \sum_{\substack{x_i=1 \\ \mathbf{x}\equiv 0 \,(\mathrm{mod}\, p)}}^{p^3} \frac{p^n}{p^{3n}}\alpha(\mathbf{x}) \\
&= \frac{1}{p^{2n}} \sum_{\mathbf{x}\equiv 0 \,(\mathrm{mod}\, p)} \alpha(\mathbf{x}) \\
&= \frac{1}{p^{2n}} \sum_{\substack{\mathbf{u}\in\mathscr{B} \\ \mathbf{u}+\mathbf{v}\equiv 0(\mathrm{mod}\, p)}} \sum_{\mathbf{v}\in\mathscr{B}} 1 \\
&\leq \frac{1}{p^{2n}} \prod_{i=1}^{n} m_i \left(\left[\frac{m_i}{p} \right] + 1 \right). \qquad (3.34)
\end{aligned}
$$

The last inequality in (3.34) is true by the same reason given in the proof of the Lemma 3.4. Now we split the product in (3.34) to get

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

and thus deduce

$$
\sum_{y_i=1}^{p} a(p^2\mathbf{y}) \leq \frac{1}{p^{2n}} |\mathscr{B}| \prod_{m_i\geq p} \frac{2m_i}{p},
$$

finishing the proof. □

By the fundamental identity (3.30) and the fact that all $a(\mathbf{y})$ are positive we have

$$
\begin{aligned}
\sum_{\mathbf{x}\in V_{p^3}} \alpha(\mathbf{x}) \geq & \underbrace{p^{-3} \sum_{\mathbf{x}} \alpha(\mathbf{x})}_{\text{Main Term}} \\
& \underbrace{- p^{(3n/2)-1} \sum_{\substack{y_i'=1 \\ p^2 | Q^*(\mathbf{y}')}}^{p^3} a(\mathbf{y}')}_{Er_4} \underbrace{- p^{2n-2} \sum_{\substack{y_i'=1 \\ p | Q^*(\mathbf{y}')}}^{p^2} a(p\mathbf{y}')}_{Er_5} \underbrace{- p^{5n/2-3} \sum_{y_i'=1}^{p} a(p^2\mathbf{y}')}_{Er_6}. \qquad (3.35)
\end{aligned}
$$

Now let us estimate the error terms Er_4, Er_5 and Er_6 in (3.35). From Lemma 3.4 and Lemma 3.5, it is follows readily that

$$
Er_5 \leq p^{2n-2} \sum_{y_i'=1}^{p^2} a(p\mathbf{y}') \leq p^{n-2} |\mathscr{B}| \prod_{m_i\geq p^2} \frac{2m_i}{p^2}.
$$

And

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

Before embarking on the estimation of the error term Er_4, it is useful to establish an analogue of Lemma 2.7 of Chapter 2.

Lemma 3.6. *Let* $V_{p^2,\mathbb{Z}} = V_{p^2,\mathbb{Z}}(Q)$ *be the set of integer solutions of the congruence* (3.5) *and let* $\Delta_p = \pm 1$. *Then for any box* $\mathscr{B}$ *of type* (3.31),

$$\left|\mathscr{B} \bigcap V_{p^2,\mathbb{Z}}\right| \le \gamma_n\left(\frac{|\mathscr{B}|}{p^2} + N_{\mathscr{B}}\ p^n\right), \tag{3.36}$$

where we define

$$N_{\mathscr{B}} = \prod_{i=1}^{n}\left(\left[\frac{m_i}{p^2}\right]+1\right). \tag{3.37}$$

Proof. Partition $\mathscr{B}$ into $N = N_{\mathscr{B}}$ smaller boxes B_i,

$$\mathscr{B} = \mathrm{B}_1 \bigcup \mathrm{B}_2 \bigcup \cdots \bigcup \mathrm{B}_N,$$

where each B_i has all of its edge lengths $\le p^2$. Then we can apply Lemma 3.2 to each B_i, to get

$$\begin{aligned}\left|\mathscr{B} \bigcap V_{p^2,\mathbb{Z}}\right| &= \sum_{i=1}^{N}\left|\,\mathrm{B}_i \bigcap V_{p^2}\,\right| \\ &\overset{\text{(Lemma 3.2)}}{\uparrow} \\ &\le \sum_{i=1}^{N}\gamma_n\left(\frac{|\mathrm{B}_i|}{p^2} + p^n\right) \\ &= \frac{\gamma_n}{p^2}\sum_{i=1}^{N}|\mathrm{B}_i| + N\gamma_n p^n \\ &= \gamma_n\left(\frac{|\mathscr{B}|}{p^2} + N_{\mathscr{B}}\ p^n\right).\end{aligned}$$

The proof of Lemma 3.6 is complete. □

Keeping in mind the above lemma, we begin bounding the error term Er_4.

$$Er_4 = p^{(3n/2)-1}\sum_{\substack{y_i'=1 \\ p^2 \mid Q^*(\mathbf{y}')}}^{p^3} a(\mathbf{y}') \le p^{(3n/2)-1}\sum_{\substack{\mathbf{y}' \,(\mathrm{mod}\, p^3) \\ Q^*(\mathbf{y}') \equiv 0 \,(\mathrm{mod}\, p^2)}} \left|a(\mathbf{y}')\right|. \tag{3.38}$$

So we shall estimate the sum $\sum_{\mathbf{y}' \,(\mathrm{mod}\, p^3),\, Q^*(\mathbf{y}') \equiv 0 \,(\mathrm{mod}\, p^2)} \left|a(\mathbf{y}')\right|$ and for brevity we shall write $\sum_{\mathbf{y} \,(\mathrm{mod}\, p^3),\, Q^*(\mathbf{y}) \equiv 0 \,(\mathrm{mod}\, p^2)} = \sum^*$. Define ρ_i as in (2.38) of Chapter 2.

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

Using the fact that

$$a(\mathbf{y}) = p^{-3n} \prod_{i=1}^{n} \left| \frac{\sin^2 \pi m_i y_i / p^3}{\sin^2 \pi y_i / p^3} \right| \leq p^{-3n} \prod_{i=1}^{n} \min \left\{ m_i^2, \left(\frac{p^3}{2y_i} \right)^2 \right\}.$$

Then

$$\begin{aligned} \sum_{\substack{\mathbf{y} \,(\mathrm{mod}\, p^3) \\ Q^*(\mathbf{y}) \equiv 0 \,(\mathrm{mod}\, p^2)}} |a(\mathbf{y})| &\leq \sum_{k_1=0}^{\infty} \cdots \sum_{k_n=0}^{\infty} \sum_{\substack{\mathbf{y} \\ \rho_i p^3 / m_i \leq |y_i| \leq 2^{k_i} p^3 / m_i}}^{*} \prod_{i=1}^{n} \min \left\{ \frac{m_i^2}{p^3}, \frac{p^3}{4y_i^2} \right\} \\ &\leq \sum_{k_1=0}^{\infty} \cdots \sum_{k_n=0}^{\infty} \sum_{\substack{\mathbf{y} \\ |y_i| \leq 2^{k_i} p^3 / m_i}}^{*} \prod_{i=1}^{n} \frac{p^3}{4(2^{k_i-1} p^3 / m_i)^2} \\ &= \frac{|\mathscr{B}|^2}{p^{3n}} \sum_{k_1=0}^{\infty} \cdots \sum_{k_n=0}^{\infty} \sum_{\substack{\mathbf{y} \\ |y_i| \leq 2^{k_i} p^3 / m_i}}^{*} \prod_{i=1}^{n} \frac{1}{2^{2k_i}}. \end{aligned} \tag{3.39}$$

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

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

Set

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

Then it follows that

$$|\mathscr{B}'| = \prod_{i=1}^{n} m_i' \leq \prod_{i=1}^{n} \left(\frac{2^{k_i+1} p^3}{m_i} + 1 \right) \leq \prod_{i=1}^{n} \frac{2^{k_i+2} p^3}{m_i}. \tag{3.40}$$

By the inequality (3.36) in Lemma 3.6, we have the upper bound

$$\left| \mathscr{B}' \cap V_{p^2, \mathbb{Z}} \right| \leq \gamma_n \frac{|\mathscr{B}'|}{p^2} + \gamma_n N_{\mathscr{B}'} \, p^n, \tag{3.41}$$

where by (3.37),

$$N_{\mathscr{B}'} = \prod_{i=1}^{n} \left(\left[\frac{m_i'}{p^2} \right] + 1 \right) = \prod_{\substack{i=1 \\ 2^{k_i} \geq m_i / 4p}}^{n} \left(\left[\frac{m_i'}{p^2} \right] + 1 \right). \tag{3.42}$$

The equality in (3.42) 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 (3.42), is less than or equal to

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

So that

$$N_{\mathscr{B}'}\leq 2^n\prod_{\substack{i=1\\ 2^{k_i}\geq m_i/4p}}^{n}\left(\frac{2^{k_i}p}{m_i}+1\right). \tag{3.43}$$

Apply the upper bound (3.40) to the inner sum $\sum_{\mathbf{y}}^{*}$ in (3.39), to obtain

$$\begin{aligned}\sum_{\substack{Q^*(\mathbf{y})\equiv 0(\mathrm{mod}\,p^2)\\ |y_i|\leq p^2/2}}|a(\mathbf{y})| &= \frac{|\mathscr{B}|^2}{p^{3n}}\sum_{k_1=0}^{\infty}\cdots\sum_{k_n=0}^{\infty}\left|\mathscr{B}'\bigcap V_{p^2,\mathbb{Z}}\right|\prod_{i=1}^{n}\frac{1}{2^{2k_i}}\\ &\leq \frac{|\mathscr{B}|^2}{p^{3n}}\sum_{k_1=0}^{\infty}\cdots\sum_{k_n=0}^{\infty}\left(\gamma_n\frac{|\mathscr{B}'|}{p^2}+\gamma_n N_{\mathscr{B}'}\ p^n\right)\prod_{i=1}^{n}\frac{1}{2^{2k_i}}\\ &\leq \varrho_1+\varrho_2, \end{aligned}\tag{3.44}$$

say. Then by the inequality (3.40),

$$\begin{aligned}\varrho_1 &= \frac{|\mathscr{B}|^2}{p^{3n}}\sum_{k_1=0}^{\infty}\cdots\sum_{k_n=0}^{\infty}\left(\prod_{i=1}^{n}\frac{1}{2^{2k_i}}\right)\gamma_n\frac{\prod_{i=1}^{n}\frac{2^{k_i+2}p^3}{m_i}}{p^2}\\ &\leq \frac{|\mathscr{B}|^2}{p^{3n}}\frac{\gamma_n}{p^2}\sum_{k_1=0}^{\infty}\cdots\sum_{k_n=0}^{\infty}\left(\prod_{i=1}^{n}\frac{1}{2^{2k_i}}\frac{2^{k_i+2}p^3}{m_i}\right)\\ &\leq 4^n\gamma_n\frac{|\mathscr{B}|^2}{p^{3n+2}}\frac{p^{3n}}{|\mathscr{B}|}\prod_{i=1}^{n}\left(\sum_{k_i}\frac{1}{2^{k_i}}\right)\\ &= 2^{3n}\gamma_n\frac{|\mathscr{B}|}{p^2}, \end{aligned}\tag{3.45}$$

and by the inequality (3.43),

$$\begin{aligned}\varrho_2 &= \frac{|\mathscr{B}|^2}{p^{3n}}\sum_{k_1=0}^{\infty}\cdots\sum_{k_n=0}^{\infty}\gamma_n N_{\mathscr{B}'}p^n\prod_{i=1}^{n}\frac{1}{2^{2k_i}}\\ &= 2^n\gamma_n\frac{|\mathscr{B}|^2}{p^{3n}}p^n\sum_{k_1=0}^{\infty}\cdots\sum_{k_n=0}^{\infty}\prod_{\substack{i=1\\ 2^{k_i}\geq m_i/4p}}^{n}\left(\frac{2^{k_i}p}{m_i}+1\right)\prod_{i=1}^{n}\frac{1}{2^{2k_i}}\\ &= 2^n\gamma_n\frac{|\mathscr{B}|^2}{p^{3n}}p^n\prod_{i=1}^{n}\left[\sum_{\substack{k_i=0\\ 2^{k_i}<m_i/4p}}^{\infty}\frac{1}{2^{2k_i}}+\sum_{\substack{k_i\\ 2^{k_i}\geq m_i/4p}}\left(\frac{2^{k_i}p}{m_i}+1\right)\frac{1}{2^{2k_i}}\right]\end{aligned}$$

$$
\begin{aligned}
&\leq 2^n \gamma_n \frac{|\mathscr{B}|^2}{p^{2n}} \prod_{i=1}^{n} \left[\sum_{k_i=0}^{\infty} \frac{1}{2^{2k_i}} + \sum_{\substack{k_i \\ 2^{k_i} \geq m_i/4p}} \frac{p}{2^{k_i} m_i} \right] \\
&= 2^n \gamma_n \frac{|\mathscr{B}|^2}{p^{2n}} \prod_{i=1}^{n} \left[\frac{4}{3} + \frac{2p^2}{m_i} \right]. \\
&\leq 2^n \gamma_n \frac{|\mathscr{B}|^2}{p^{2n}} \prod_{i=1}^{n} \left(\frac{4}{3} + \frac{2p}{m_i} \right) \\
&\leq 2^n \gamma_n \frac{|\mathscr{B}|^2}{p^{2n}} \left(\prod_{m_i \leq p} \frac{4p}{m_i} \right) \left(\prod_{m_i > p} \frac{10}{3} \right) \\
&\leq 8^n \gamma_n \frac{|\mathscr{B}|^2}{p^{2n}} \prod_{m_i \leq p} \frac{p}{m_i}. \qquad (3.46)
\end{aligned}
$$

Thus by inequalities (3.38), (3.44), (3.45) and (3.46), we have

$$
\begin{aligned}
Er_4 &\leq p^{(3n/2)-1} \left[2^{3n} \gamma_n \frac{|\mathscr{B}|}{p^2} \right] + p^{(3n/2)-1} \left[8^n \gamma_n \frac{|\mathscr{B}|^2}{p^{2n}} \prod_{m_i \leq p} \frac{p}{m_i} \right] \\
&= \underbrace{2^{3n} \gamma_n p^{(3n/2)-3} |\mathscr{B}|}_{Er_{4,1}} + \underbrace{8^n \gamma_n \frac{|\mathscr{B}|^2}{p^{(n/2)+1}} \prod_{m_i \leq p} \frac{p}{m_i}}_{Er_{4,2}}. \qquad (3.47)
\end{aligned}
$$

Summarizing our findings we obtain

Theorem 3.1. *Assume that $n \geq 4$ is even, and that $\Delta_p(Q) = +1$. Then for any $\mathscr{B}$ box centered at the origin,*

$$
\sum_{\mathbf{x} \in V} \alpha(\mathbf{x}) \geq \frac{|\mathscr{B}|^2}{p^3} - |Error|,
$$

where

$$
\begin{aligned}
|Error| < &\underbrace{2^{3n} \gamma_n p^{(3n/2)-3} |\mathscr{B}|}_{Er_{4,1}} + \underbrace{\gamma_n 8^n \frac{|\mathscr{B}|^2}{p^{(n/2)+1}} \prod_{m_i \leq p} \frac{p}{m_i}}_{Er_{4,2}} \\
&+ \underbrace{p^{n-2} |\mathscr{B}| \prod_{m_i \geq p^2} \frac{2m_i}{p^2}}_{Er_5} + \underbrace{p^{(n/2)-3} |\mathscr{B}| \prod_{m_i \geq p}^{n} \frac{2m_i}{p}}_{Er_6}.
\end{aligned}
$$

Here we have indicated below each term, the error term bounded by the given value.

In what follows we compare each error term in Theorem 3.1 to the

main term $|\mathscr{B}|^2/p^3$. 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 of the main term. For the error term $Er_{4,1}$, we need

$$\frac{1}{5}\frac{|\mathscr{B}|^2}{p^3} \geq 2^{3n}\gamma_n p^{(3n/2)-3}|\mathscr{B}| \Longleftrightarrow |\mathscr{B}| \geq 5\cdot 2^{3n}\gamma_n p^{3n/2}. \tag{3.48}$$

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

$$\frac{1}{5}\frac{|\mathscr{B}|^2}{p^3} \geq \gamma_n 8^n \frac{|\mathscr{B}|^2}{p^{(n/2)+1}}\prod_{m_i\leq p}\frac{p}{m_i} \iff p^{(n/2)-2} \geq 5\gamma_n 8^n \prod_{m_i<p}\frac{p^2}{m_i}. \tag{3.49}$$

For the error term Er_5, we require that

$$\frac{1}{5}\frac{|\mathscr{B}|^2}{p^3} \geq p^{n-2}|\mathscr{B}|\prod_{m_i\geq p^2}^{n}\frac{2m_i}{p^2} \Longleftrightarrow |\mathscr{B}| \geq 5p^{n+1}\prod_{m_i\geq p^2}\frac{2m_i}{p^2}. \tag{3.50}$$

Finally, for the error term Er_6,

$$\frac{1}{5}\frac{|\mathscr{B}|^2}{p^3} \geq p^{(n/2)-3}|\mathscr{B}|\prod_{m_i\geq p}\frac{2m_i}{p} \Longleftrightarrow |\mathscr{B}| \geq 5p^{n/2}\prod_{m_i\geq p}\frac{2m_i}{p}. \tag{3.51}$$

If the inequalities in (3.48), (3.49), (3.50) and (3.51) hold, then there exist solutions for the congruence (3.1)

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

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

Theorem 3.2. *Suppose that $n \geq 6$ is even, and that $\Delta_p(Q) = +1$. If* (3.48), (3.49), (3.50) *and* (3.51) *hold, then*

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

In particular

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

The condition $n \geq 6$ is placed in Theorem 3.2 because when $n = 4$ condition (3.49) always fails. The next corollary demonstrates the existence of a primitive solution of the congruence (3.1).

Corollary 3.1. *Make the hypotheses of Theorem* 3.2*, and assume that $n \geq 6$. Then $\mathscr{B}+\mathscr{B}$ contains a primitive solution of* (3.1).

Proof. First, recall that a solution of (3.1) 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 3.5, we can write

$$\sum_{\substack{\mathbf{x}\in V\\ p|\mathbf{x}}}\alpha(\mathbf{x}) \le \sum_{\substack{p|x_i,\\ 1\le i\le n}}\alpha(\mathbf{x}) = \sum_{\substack{\mathbf{u}\in\mathscr{B}\\ \mathbf{u}+\mathbf{v}\equiv 0(\mathrm{mod}\,p)}}\sum_{\mathbf{v}\in\mathscr{B}} 1 \le \prod_{i=1}^{n} m_i\left(\left[\frac{m_i}{p}\right]+1\right) \le |\mathscr{B}|\prod_{m_i\ge p}\frac{2m_i}{p}. \tag{3.52}$$

We claim that the latter quantity is less than $|\mathscr{B}|^2/5p^3$ for $n\ge 6$. Indeed, by our hypothesis (3.51), which says

$$|\mathscr{B}| \ge 5p^{n/2}\prod_{m_i\ge p}\frac{2m_i}{p} \quad\Longleftrightarrow\quad \prod_{m_i\ge p}\frac{2m_i}{p} \le \frac{|\mathscr{B}|}{5p^{n/2}}.$$

Since $n\ge 6$, the latter quantity is $\le |\mathscr{B}|/5p^3$. On the other hand Theorem 3.2 yields,

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

We therefore obtain

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

completing our proof. □

§3.4. Special case that $\mathscr{B}$ is a cube, $\Delta = +1$.

In connection with Theorem 3.2 we study the following special case when the box $\mathscr{B}$ is a cube.

Corollary 3.2. *Suppose* $n\ge 6$ *and* $p > 5^{2/(n-4)}2^{10n/(n-4)}\gamma_n^{2/(n-4)}$ (*where* γ_n *is given in* (3.6)). *Let* $\mathscr{B}$ *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* $\mathscr{B}+\mathscr{B}$ *contains a primitive solution of* (3.1).

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 3.2 are satisfied. Indeed,

$$(3.48) \iff B^n > 5 \cdot 2^{3n} \gamma_n p^{3n/2} \iff B > 5^{1/n} 2^3 \gamma_n^{1/n} p^{3/2}.$$

For the hypothesis,

$$\begin{aligned}(3.49) &\iff 5^{-1}(32)^{-n} \gamma_n^{-1} p^{(n/2)-2} \geq \prod_{m_i < p} \frac{p^2}{m_i} \prod_{p < m_i < p^{3/2}} \frac{p^3}{m_i^2} = 1 \cdot 1 \\ &\iff n \geq 6 \text{ and } p > 5^{2/(n-4)} (32)^{2n/(n-4)} \gamma_n^{2/(n-4)}.\end{aligned}$$

Next, for the condition,

$$\begin{aligned}(3.50) \iff B^n > 5p^{n+1} \prod_{m_i \geq p^2} \frac{2m_i}{p^2} &\iff B^n > 5p^{n+1}, \text{ since } B < p^2 \\ &\iff B > 5^{1/n} p^{1+(1/n)}.\end{aligned}$$

Lastly, for

$$(3.51) \iff B^n \geq 5p^{n/2} \prod_{m_i \geq p} \frac{2m_i}{p} = 5p^{n/2} \frac{2^n B^n}{p^n} \iff p > 4 \cdot 5^{2/n}.$$

Thus the hypotheses of Theorem 3.2 are satisfied, and so Corollary 3.1 applies.

§3.5. Bounds on the error terms in the fundam -ental identity (mod p^3).The case of $\Delta = -1$.

Letting $\Delta = -1$ in (3.2), we obtain

$$\begin{aligned}\sum_{\mathbf{x} \in V_{p^3}} \alpha(\mathbf{x}) &= p^{-3} \sum_{\mathbf{x}} \alpha(\mathbf{x}) \\ &- \underbrace{p^{3n/2} \sum_{\substack{y_i' = 1 \\ p^3 | Q^*(\mathbf{y}')}}^{p^3} a(\mathbf{y}')}_{Er_1} + \underbrace{p^{2n-1} \sum_{\substack{y_i' = 1 \\ p^2 | Q^*(\mathbf{y}')}}^{p^2} a(p\mathbf{y}')}_{Er_2} - \underbrace{p^{5n/2-2} \sum_{\substack{y_i' = 1 \\ p | Q^*(\mathbf{y}')}}^{p} a(p^2\mathbf{y}')}_{Er_3} \\ &+ \underbrace{p^{(3n/2)-1} \sum_{\substack{y_i' = 1 \\ p^2 | Q^*(\mathbf{y}')}}^{p^3} a(\mathbf{y}')}_{Er_4} - \underbrace{p^{2n-2} \sum_{\substack{y_i' = 1 \\ p | Q^*(\mathbf{y}')}}^{p^2} a(p\mathbf{y}')}_{Er_5} + \underbrace{p^{5n/2-3} \sum_{y_i' = 1}^{p} a(p^2\mathbf{y}')}_{Er_6}. \quad (3.53)\end{aligned}$$

Letting $\alpha(\mathbf{y}) = \chi_{\mathscr{B}} * \chi_{\mathscr{B}}$ as before, so that all the $a(\mathbf{y})$ are positive we see

$$\sum_{\mathbf{x}\in V_{p^3}} \alpha(\mathbf{x}) \geq \underbrace{p^{-3}\sum_{\mathbf{x}} \alpha(\mathbf{x})}_{\text{Main Term}} - \underbrace{p^{3n/2} \sum_{\substack{y_i'=1 \\ p^3|Q^*(\mathbf{y}')}}^{p^3} a(\mathbf{y}')}_{Er_1} - \underbrace{p^{5n/2-2} \sum_{\substack{y_i'=1 \\ p|Q^*(\mathbf{y}')}}^{p} a(p^2\mathbf{y}')}_{Er_3} - \underbrace{p^{2n-2} \sum_{\substack{y_i'=1 \\ p|Q^*(\mathbf{y}')}}^{p^2} a(p\mathbf{y}')}_{Er_5}. \tag{3.54}$$

Let us now bounded the error terms in (3.54). The error terms Er_3 and Er_5 can be bounded easily by using Lemma 3.5 and Lemma 3.4. We obtain

$$Er_3 \leq p^{(5n/2)-2}\sum_{y'=1}^{p} a(p^2\mathbf{y}') \overset{\text{Lemma 3.5}}{\uparrow} \leq p^{(5n/2)-2}\,\frac{|\mathscr{B}|}{p^{2n}} \prod_{m_i\geq p}\frac{2m_i}{p} = p^{(n/2)-2}\,|\mathscr{B}| \prod_{m_i\geq p}\frac{2m_i}{p}.$$

$$Er_5 \leq p^{2n-2}\sum_{y_i'=1}^{p^2} a(p\,\mathbf{y}') \overset{\text{Lemma 3.4}}{\uparrow} \leq p^{2n-2}\,\frac{|\mathscr{B}|}{p^{n}} \prod_{m_i\geq p^2}\frac{2m_i}{p^2} = p^{n-2}\,|\mathscr{B}| \prod_{m_i\geq p^2}\frac{2m_i}{p^2}.$$

To estimate the error term Er_1 we need to construct a lemma like Lemma 3.1. We shall prove the Lemma for both the cases $\Delta = +1$ and $\Delta = -1$ although for this section we just need $\Delta = -1$.

Lemma 3.7. *Let p be an odd prime, $V_{p^3} = V_{p^3}(Q)$ be the set of zeros of (3.4) in $\mathbb{Z}_{p^3}^n$, and $\mathscr{B}$ be a box as given in (3.3) centered at the origin with all $m_i \leq p^3$. Then*

$$\left|\mathscr{B} \bigcap V_{p^3}\right| \leq \begin{cases} \eta_n\left(\dfrac{|\mathscr{B}|}{p^3} + p^{3n/2-1}\right) & \text{if } \Delta = -1, \\ \eta_n\left(\dfrac{|\mathscr{B}|}{p^3} + p^{3n/2}\right) & \text{if } \Delta = +1, \end{cases} \tag{3.55}$$

where

$$\eta_n = \begin{cases} 2^n\left(1 + 2^n + \dfrac{2^{(n/2)+1}}{p}\right), & \Delta = -1, \\ 2^n\left(1 + 2^n + 2^{(n/2)+1}\right), & \Delta = +1. \end{cases} \tag{3.56}$$

Proof. Consider (3.2), the fundamental identity (mod p^3). Put $\alpha = \chi_{\mathscr{B}} * \chi_{\mathscr{B}} = \sum_{\mathbf{y}} a(\mathbf{y}) e_{p^3}(\mathbf{x}\cdot\mathbf{y})$. Then the Fourier coefficients of $\alpha(\mathbf{x})$ are given by $a(\mathbf{y}) = p^{3n} a_{\mathscr{B}}^2(\mathbf{y})$ and by Parseval's identity satisfy

$$\sum_{\mathbf{y}} \left|a(\mathbf{y})\right| = p^{3n} \sum_{\mathbf{y}} \left|a_{\mathscr{B}}(\mathbf{y})\right|^2 = \sum_{\mathbf{y}} \left|\chi_{\mathscr{B}}(\mathbf{y})\right|^2 = |\mathscr{B}|. \tag{3.57}$$

Consequently from (3.57), the error term Er_4 in (3.2) can be bounded by

$$p^{3n/2-1} \sum_{\substack{y_i' \\ p^2 | Q^*(\mathbf{y})}}^{p^3} a(\mathbf{y}') \le p^{3n/2-1} \sum_{\mathbf{y}} \left|a(\mathbf{y}')\right| \le p^{3n/2-1} |\mathscr{B}|. \tag{3.58}$$

Besides this we have that the main term in (3.2) is

$$p^{-3} \sum_{\mathbf{x}} \alpha(\mathbf{x}) = p^{-2} \sum_{\mathbf{x}} \chi_{\mathscr{B}} * \chi_{\mathscr{B}}(\mathbf{x}) = \frac{|\mathscr{B}|^2}{p^3}. \tag{3.59}$$

Also we have by Lemma 3.4,

$$p^{2n-1} \sum_{\substack{y_i' = 1 \\ p^2 | Q^*(y')}}^{p^2} a(p\mathbf{y}') \le p^{2n-1} \frac{|\mathscr{B}|}{p^n} \prod_{m_i \ge p^2} \frac{2m_i}{p^2} = p^{n-1} |\mathscr{B}| \prod_{m_i \ge p^2} \frac{2m_i}{p^2}, \tag{3.60}$$

and by Lemma 3.5,

$$p^{(5n/2)-3} \sum_{y_i=1}^{p} a(p^2\mathbf{y}') \le p^{(5n/2)-3} \frac{|\mathscr{B}|}{p^{2n}} \prod_{m_i \ge p} \frac{2m_i}{p} = p^{(n/2)-3} |\mathscr{B}| \prod_{m_i \ge p} \frac{2m_i}{p}. \tag{3.61}$$

Now turn back to (3.53), if $\Delta = -1$, we have

$$\begin{aligned} \sum_{\mathbf{x} \in V_{p^3}} \alpha(\mathbf{x}) &\le p^{-3} \sum_{\mathbf{x}} \alpha(\mathbf{x}) \\ &\quad + p^{(3n/2)-1} \sum_{\substack{y_i' = 1 \\ p^2 | Q^*(\mathbf{y}')}}^{p^3} a(\mathbf{y}') + p^{2n-1} \sum_{\substack{y_i' = 1 \\ p^2 | Q^*(\mathbf{y}')}}^{p^2} a(p\mathbf{y}') + p^{5n/2-3} \sum_{y_i'=1}^{p} a(p^2\mathbf{y}') \end{aligned} \tag{3.62}$$

Then by inequalities in (3.59), (3.58), (3.60), and (3.61) we obtain

$$\sum_{\mathbf{x} \in V_{p^3}} \alpha(\mathbf{x}) \le \frac{|\mathscr{B}|^2}{p^3} + p^{3n/2-1} |\mathscr{B}| + p^{n-1} |\mathscr{B}| \prod_{m_i \ge p^2} \frac{2m_i}{p^2} + p^{n/2-3} |\mathscr{B}| \prod_{m_i \ge p} \frac{2m_i}{p}. \tag{3.63}$$

But, as in the proof (2.23) in Lemma 2.5 of Chapter 2, we have

$$\sum_{\mathbf{x}\in V_{p^3}} \alpha(\mathbf{x}) \geq \frac{1}{2^n}|\mathscr{B}|\Big|V_{p^3} \bigcap \mathscr{B}\Big|. \tag{3.64}$$

Thus we have

$$\Big|V_{p^3} \bigcap \mathscr{B}\Big| \leq 2^n \left(\underbrace{\frac{|\mathscr{B}|}{p^3}}_{❶} + \underbrace{p^{(3n/2)-1}}_{❷} + \underbrace{p^{n-1} \prod_{m_i \geq p^2} \frac{2m_i}{p^2}}_{❸} + \underbrace{p^{(n/2)-3} \prod_{m_i \geq p} \frac{2m_i}{p}}_{❹} \right). \tag{3.65}$$

The task now is designation which of the terms ❶, ❷, ❸ and ❹ in (3.65) is the dominant term. We consider two cases:

***Case* (i):** We define l by

$$m_1 \leq m_2 \leq \cdots \leq m_l < p^2 \leq m_{l+1} \leq \cdots \leq m_n .$$

Then

I. Assume $l \leq \frac{n}{2} - 1$. Then compare

$$\frac{❸}{❶} = \frac{p^{n-1} \prod_{m_i \geq p^2} \frac{2m_i}{p^2}}{\frac{1}{p^3} \prod_{i=1}^{n} m_i} = \frac{2^{n-l} p^{n+2}}{p^{2(n-l)} \prod_{m_i < p^2} m_i} = \frac{2^{n-l}}{p^{n-2l-2} \prod_{m_i < p^2} m_i} \leq \frac{2^{n-l}}{1 \cdot 1} \leq 2^n,$$

which leads to

$$❸ \leq 2^n \; ❶ \quad \text{or} \quad p^{n-1} \prod_{m_i \geq p^2}^{n} \frac{2m_i}{p^2} \leq 2^n \frac{|\mathscr{B}|}{p^3}.$$

II. Assume $l \geq \frac{n}{2}$. Then compare

$$\frac{❸}{❷} = \frac{p^{n-1} \prod_{m_i \geq p^2} \frac{2m_i}{p^2}}{p^{(3n/2)-1}} = \frac{1}{p^{n/2}} \prod_{m_i \geq p^2} \frac{2m_i}{p^2} \leq \frac{1}{p^{n/2}} \prod_{m_i \geq p^2} 2p \leq \frac{1}{p^{n/2}} (2p)^{n/2} = 2^{n/2},$$

which implies that

$$❸ \leq 2^{n/2} \; ❷ \quad \text{or} \quad p^{n-1} \prod_{m_i \geq p^2}^{n} \frac{2m_i}{p^2} \leq 2^{n/2} p^{(3n/2)-1}.$$

We get by (I) and (II) that

$$❸ \leq \max\left(2^n ❶ \, , 2^{n/2} ❷\right) \leq 2^n ❶ + 2^{n/2} ❷ .$$

***Case* (ii):** We define l' by

$$m_1 \leq m_2 \leq \cdots \leq m_{l'} < p \; \leq m_{l'+1} \leq \cdots \leq m_n .$$

Then

III. Assume $l' \leq \frac{n}{2} - 1$. Then compare

$$\frac{❹}{❶} = \frac{p^{(n/2)-3}\prod_{m_i\geq p}\frac{2m_i}{p}}{\frac{1}{p^3}\prod_{i=1}^{n} m_i} = \frac{2^{n-l'}p^{n/2}}{p^{n-l'}\prod_{m_i<p} m_i} = \frac{2^{n-l'}}{p^{(n/2)-l'}\prod_{m_i<p} m_i} \leq \frac{2^n}{p^{n/2}}\left(\frac{p}{2}\right)^{l'}$$
$$\leq \frac{2^n}{p^{n/2}}\left(\frac{p}{2}\right)^{(n/2)-1} \leq \frac{2^{(n/2)+1}}{p},$$

leads to

$$❹ \leq \frac{2^{(n/2)+1}}{p}\,❶ \quad \text{or} \quad p^{n/2-3}\prod_{m_i\geq p}^{n}\frac{2m_i}{p} \leq \frac{2^{(n/2)+1}}{p}\frac{|\mathscr{B}|}{p^3}.$$

IV. Assume $l' \geq \frac{n}{2}$. Then compare

$$\frac{❹}{❷} = \frac{p^{(n/2)-3}\prod_{m_i\geq p}\frac{2m_i}{p}}{p^{(3n/2)-1}} = \frac{1}{p^{n+2}}\prod_{m_i\geq p}\frac{2m_i}{p} \leq \frac{1}{p^{n+2}}\prod_{m_i\geq p} 2p^2 \leq \frac{1}{p^{n+2}}(2p^2)^{n-l'}$$
$$\leq \frac{1}{p^{n+2}}(2p^2)^{n/2} = \frac{2^{n/2}}{p^2},$$

implies that

$$❹ \leq \frac{2^{n/2}}{p^2}\,❷ \quad \text{or} \quad p^{n/2-3}\prod_{m_i\geq p}^{n}\frac{2m_i}{p} \leq \frac{2^{n/2}}{p^2}p^{(3n/2)-1}.$$

Thus by (III) and (IV),

$$❹ \leq \frac{2^{(n/2)+1}}{p}\,❶ + \frac{2^{n/2}}{p^2}\,❷.$$

Together, ***case* (i)** and ***case* (ii)** gives us

$$❸ + ❹ \leq \left(2^n + \frac{2^{(n/2)+1}}{p}\right)❶ + \left(2^{n/2} + \frac{2^{n/2}}{p^2}\right)❷$$

We conclude by making use of (3.65) to get

$$\begin{aligned}\left|V_{p^3}\cap\mathscr{B}\right| &\leq 2^n\big(❶ + ❷ + ❸ + ❹\big)\\ &\leq 2^n\left\{❶ + ❷ + \left(2^n + \frac{2^{(n/2)+1}}{p}\right)❶ + \left(2^{n/2} + \frac{2^{n/2}}{p^2}\right)❷\right\}\\ &= 2^n\left\{\left[❶ + \left(2^n + \frac{2^{(n/2)+1}}{p}\right)❶\right] + \left[❷ + \left(2^{n/2} + \frac{2^{n/2}}{p^2}\right)❷\right]\right\}\\ &= 2^n\left(1 + 2^n + \frac{2^{(n/2)+1}}{p}\right)❶ + 2^n\left(1 + 2^{n/2} + \frac{2^{n/2}}{p^2}\right)❷\\ &\leq \eta_n'\left(\frac{|\mathscr{B}|}{p^2} + p^{(3n/2)-1}\right),\end{aligned}$$

where $\eta_n' = 2^n\left(1 + 2^n + \frac{2^{(n/2)+1}}{p}\right)$.

We now examine the case $\Delta = +1$. Appealing, once more, to (3.2), we obtain

$$\sum_{\mathbf{x}\in V_{p^3}} \alpha(\mathbf{x}) \le p^{-3}\sum_{\mathbf{x}} \alpha(\mathbf{x})$$
$$+ p^{3n/2} \sum_{\substack{y'=1 \\ p^3 | Q^*(\mathbf{y}')}}^{p^3} a(\mathbf{y}') + p^{2n-1} \sum_{\substack{y'=1 \\ p^2 | Q^*(\mathbf{y}')}}^{p^2} a(p\mathbf{y}') + p^{5n/2-2} \sum_{\substack{y'=1 \\ p | Q^*(\mathbf{y}')}}^{p} a(p^2\mathbf{y}')$$
$$\le \underbrace{\frac{|\mathscr{B}|^2}{p^3}}_{\text{by (3.59)}} + \underbrace{p^{3n/2}|\mathscr{B}|}_{\text{by (3.57)}} + \underbrace{p^{2n-1}\frac{|\mathscr{B}|}{p^n}\prod_{m_i\ge p^2}\frac{2m_i}{p^2}}_{\text{by (3.60)}} + \underbrace{p^{(5n/2)-2}\frac{|\mathscr{B}|}{p^{2n}}\prod_{m_i\ge p}\frac{2m_i}{p}}_{\text{by Lemma (3.5)}}.$$

But, once again by (3.65), we obtain

$$\left|V_{p^3}\cap\mathscr{B}\right| \le 2^n\left(\underbrace{\frac{|\mathscr{B}|}{p^3}}_{❶} + \underbrace{p^{3n/2}}_{②} + \underbrace{p^{n-1}\prod_{m_i\ge p^2}\frac{2m_i}{p^2}}_{❸} + \underbrace{p^{(n/2)-2}\prod_{m_i\ge p}\frac{2m_i}{p}}_{④}\right). \tag{3.66}$$

We do a similar investigation (as before) to determine which of the quantities ❶, ②, ❸ and ④ of (3.66) is the dominant term. Indeed in ***case* (i)** when $l \le \frac{n}{2}-1$, we have (as we saw earlier) $❸ \le 2^n\ ❶$, and when $l \le \frac{n}{2}$,

$$\frac{❸}{②} = \frac{p^{n-1}\prod_{m_i\ge p^2}\frac{2m_i}{p^2}}{p^{3n/2}} = \frac{1}{p^{(n/2)+1}}\prod_{m_i\ge p^2}\frac{2m_i}{p^2} \le \frac{1}{p^{(n/2)+1}}\prod_{m_i\ge p^2}2p$$
$$\le \frac{1}{p^{(n/2)+1}}(2p)^{n/2} = \frac{2^{n/2}}{p},$$

which means $❸ \le \dfrac{2^{n/2}}{p}\ ❷$. We therefore obtain

$$❸ \le \max\left(2^n ❶\,,\ \frac{2^{n/2}}{p}\ ②\right) \le 2^n ❶ + \frac{2^{n/2}}{p}\ ②\,.$$

In ***case* (ii)** when $l' \le \frac{n}{2}-1$, we have

$$\frac{④}{❶} = \frac{p^{(n/2)-2}\prod_{m_i\ge p}\frac{2m_i}{p}}{\frac{1}{p^3}\prod_{i=1}^n m_i} = \frac{2^{n-l'}p^{(n/2)+1}}{p^{n-l'}\prod_{m_i<p} m_i} = \frac{2^{n-l'}}{p^{(n/2)-l'-1}\prod_{m_i<p} m_i}$$
$$\le \frac{2^n}{p^{(n/2)-1}}\left(\frac{p}{2}\right)^{l'} \le \frac{2^n}{p^{(n/2)-1}}\left(\frac{p}{2}\right)^{(n/2)-1} \le 2^{(n/2)+1},$$

which means $④ \le 2^{n/2+1}\ ❶$. When $l' \le \frac{n}{2}$,

$$\frac{④}{②} = \frac{p^{(n/2)-2}\prod_{m_i\geq p}\frac{2m_i}{p}}{p^{3n/2}} = \frac{1}{p^{n+2}}\prod_{m_i\geq p}\frac{2m_i}{p} \leq \frac{1}{p^{n+2}}\prod_{m_i\geq p}2p^2 \leq \frac{1}{p^{n+2}}(2p^2)^{n-l'}$$

$$\leq \frac{1}{p^{n+2}}(2p^2)^{n/2} = \frac{2^{n/2}}{p^2},$$

which means $④ \leq \frac{2^{n/2}}{p^2}\,②$. Thus we get

$$④ \leq 2^{n/2+1}\,❶ + \frac{2^{n/2}}{p^2}\,②.$$

Putting ***case* (i)** and ***case* (ii)** together, we obtain

$$❸ + ④ \leq \quad 2^n ❶ + \frac{2^{n/2}}{p}\,② + 2^{n/2+1}\,❶ + \frac{2^{n/2}}{p^2}\,②.$$

We therefore deduce by (3.66)

$$\begin{aligned}\left|V_{p^3}\cap\mathscr{B}\right| &\leq 2^n\big(❶ + ② + ❸ + ④\big)\\ &\leq 2^n\left\{❶ + ② + \left(2^n + 2^{(n/2)+1}\right)❶ + \left(\frac{2^{n/2}}{p} + \frac{2^{n/2}}{p^2}\right)②\ \right\}\\ &= 2^n\left(1 + 2^n + 2^{(n/2)+1}\right)❶ + 2^n\left(1 + \frac{2^{n/2}}{p} + \frac{2^{n/2}}{p^2}\right)②\\ &\leq \eta_n''\left(\frac{|\mathscr{B}|}{p^2} + p^{3n/2}\right),\end{aligned}$$

where $\eta_n'' = 2^n\,(1 + 2^n + 2^{(n/2)+1})$.

Lastly let $\eta_n = \eta'$ if $\Delta = -1$ and $\eta_n = \eta''$ if $\Delta = +1$ to conclude the proof of Lemma 3.7. □

We now bound Er_1 using the above Lemma. As we shall see this method leads to a poor bound. We obtain an improved bound on page 83. First, it is clear that

$$Er_1 = p^{3n/2}\sum_{\substack{y_i'=1\\ p^3\mid Q^*(\mathbf{y}')}}^{p^3} a(\mathbf{y}') \leq p^{3n/2}\sum_{\substack{\mathbf{y}'(\mathrm{mod}\,p^3)\\ Q^*(\mathbf{y}')\equiv 0\,(\mathrm{mod}\,p^3)}}\left|a(\mathbf{y}')\right|. \tag{3.67}$$

so the task become to bound the sum $\sum_{\mathbf{y}'(\mathrm{mod}\,p^3),Q^*(\mathbf{y}')\equiv 0\,(\mathrm{mod}\,p^3)}\left|a(\mathbf{y}')\right|$. For simplicity we write $\sum^*$ instead of $\sum_{\mathbf{y}(\mathrm{mod}\,p^3),Q^*(\mathbf{y})\equiv 0\,(\mathrm{mod}\,p^3)}$. Using the fact that

$$a(\mathbf{y}) \le p^{-3n}\prod_{i=1}^{n}\min\left\{m_i^2,\left(\frac{p^3}{2y_i}\right)^2\right\} = \prod_{i=1}^{n}\min\left\{\frac{m_i^2}{p^3},\frac{p^3}{4y_i^2}\right\},$$

and taking into consideration our definition for $\rho_i = 2^{k_i-1}$ when $k_i \ge 1$ and $\rho_i = 0$ when $k_i = 0$, we may write

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

$$\le \sum_{k_1=0}^{\infty}\cdots\sum_{k_n=0}^{\infty}\sum_{\substack{\mathbf{y}\\ |y_i|\le 2^{k_i}p^3/m_i}}^{*}\prod_{i=1}^{n}\frac{p^3}{4(2^{k_i-1}p^3/m_i)^2}$$

$$= \frac{|\mathscr{B}|^2}{p^{3n}}\sum_{k_1=0}^{\infty}\cdots\sum_{k_n=0}^{\infty}\sum_{\substack{\mathbf{y}\\ |y_i|\le 2^{k_i}p^3/m_i}}^{*}\prod_{i=1}^{n}\frac{1}{2^{2k_i}}\,. \tag{3.68}$$

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

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

Set

$$m_i' = 2\left\lfloor\frac{2^{k_i}p^3}{m_i}\right\rfloor + 1\,,$$

Then it follows that

$$|\mathscr{B}'| = \prod_{i=1}^{n}m_i' \le \prod_{i=1}^{n}\left(\frac{2^{k_i+1}p^3}{m_i}+1\right) \le \prod_{i=1}^{n}\frac{2^{k_i+2}p^3}{m_i}. \tag{3.69}$$

Using (3.55) in Lemma 3.7, we obtain

$$\left|\mathscr{B}'\cap V_{p^3}\right| \le \eta_n\left(\frac{|\mathscr{B}'|}{p^3} + p^{(3n/2)-1}\right). \tag{3.70}$$

Inserting the upper bound (3.70) applied to the inner sum $\sum_{\mathbf{y}}^{*}$ in (3.68), we obtain the following:

$$\sum_{\substack{Q^*(\mathbf{y})\equiv 0(\mathrm{mod}\,p^3)\\ |y_i|\le p^3/2}}|a(\mathbf{y})| = \frac{|\mathscr{B}|^2}{p^{3n}}\sum_{k_1=0}^{\infty}\cdots\sum_{k_n=0}^{\infty}\left|\mathscr{B}'\cap V_{p^3}\right|\prod_{i=1}^{n}\frac{1}{2^{2k_i}}$$

$$\le \frac{|\mathscr{B}|^2}{p^{3n}}\sum_{k_1=0}^{\infty}\cdots\sum_{k_n=0}^{\infty}\left(\eta_n\frac{|\mathscr{B}'|}{p^3}+\eta_n p^{(3n/2)-1}\right)\prod_{i=1}^{n}\frac{1}{2^{2k_i}}$$

$$\le \varsigma_1 + \varsigma_2, \text{ say.} \tag{3.71}$$

Then by the inequality (3.69),

$$\begin{aligned}
\varsigma_1 &= \frac{|\mathscr{B}|^2}{p^{3n}} \sum_{k_1=0}^{\infty} \cdots \sum_{k_n=0}^{\infty} \Big(\prod_{i=1}^{n} \frac{1}{2^{2k_i}} \Big) \eta_n \, \frac{\prod_{i=1}^{n} \frac{2^{k_i+2} p^3}{m_i}}{p^3} \\
&\le \frac{|\mathscr{B}|^2}{p^{3n}} \frac{\eta_n}{p^3} \sum_{k_1=0}^{\infty} \cdots \sum_{k_n=0}^{\infty} \Big(\prod_{i=1}^{n} \frac{1}{2^{2k_i}} \frac{2^{k_i+2} p^3}{m_i} \Big) \\
&\le 4^n \eta_n \, \frac{|\mathscr{B}|^2}{p^{3n+3}} \frac{p^{3n}}{|\mathscr{B}|} \prod_{i=1}^{n} \Big(\sum_{k_i} \frac{1}{2^{k_i}} \Big) \\
&= 2^{3n} \eta_n \, \frac{|\mathscr{B}|}{p^3} . \qquad (3.72)
\end{aligned}$$

Next for the sum ς_2:

$$\begin{aligned}
\varsigma_2 &= \frac{|\mathscr{B}|^2}{p^{3n}} \sum_{k_1=0}^{\infty} \cdots \sum_{k_n=0}^{\infty} \eta_n p^{(3n/2)-1} \prod_{i=1}^{n} \frac{1}{2^{2k_i}} \\
&= 2^n \eta_n \, \frac{|\mathscr{B}|^2}{p^{3n}} \, p^{(3n/2)-1} \sum_{k_1=0}^{\infty} \cdots \sum_{k_n=0}^{\infty} \prod_{i=1}^{n} \frac{1}{2^{2k_i}} \\
&\le 2^{2n} \eta_n \, \frac{|\mathscr{B}|^2}{p^{(3n/2)+1}} . \qquad (3.73)
\end{aligned}$$

From (3.67), (3.71), (3.72), and (3.73) it follows that

$$\begin{aligned}
Er_1 &\le p^{3n/2} \sum_{Q(\mathbf{y}) \equiv 0 (\mathrm{mod}\, p^3)} \big| a(\mathbf{y}) \big| \\
&\le p^{3n/2} \Big(2^{3n} \eta_n \, \frac{|\mathscr{B}|}{p^3} + 2^{2n} \eta_n \, \frac{|\mathscr{B}|^2}{p^{(3n/2)+1}} \Big) \\
&\le \underbrace{2^{3n} \eta_n \, |\mathscr{B}| \, p^{(3/2n)-3}}_{Er_{1,1}} + \underbrace{2^{2n} \eta_n \, \frac{|\mathscr{B}|^2}{p}}_{Er_{1,2}} .
\end{aligned}$$

Notice that the error term $Er_{1,2}$ is too big, that is, larger than the main term. This causes trouble. Thus we appeal instead to another more elementary way of bounding Er_1.

$$\sum_{Q(\mathbf{y}) \equiv 0 (\mathrm{mod}\, p^3)} \big| a(\mathbf{y}) \big| \le \sum_{\mathbf{y}} \big| a(\mathbf{y}) \big| \le |\mathscr{B}| .$$

We get the estimate

$$Er_1 \le p^{3n/2} \, |\mathscr{B}| ,$$

which settles the problem.

Summing up our investigation, we obtain

Theorem 3.3. *Assume that* $n \geq 4$ *is even, and that* $\Delta_p(Q) = -1$. *Then for any* $\mathscr{B}$ *box centered at the origin,*

$$\sum_{\mathbf{x}\in V} \alpha(\mathbf{x}) \geq \frac{|\mathscr{B}|^2}{p^3} - |Error|,$$

where

$$|Error| \leq \underbrace{p^{3n/2}|\mathscr{B}|}_{Er_1} + \underbrace{p^{(n/2)-2}|\mathscr{B}| \prod_{m_i \geq p} \frac{2m_i}{p}}_{Er_3} + \underbrace{p^{n-2}|\mathscr{B}| \prod_{m_i \geq p^2} \frac{2m_i}{p^2}}_{Er_5}.$$

We emphasize here, below each term we have indicated which error term it corresponds with.

Our next step is to make each of the error terms Er_1, Er_3, and Er_5 in Theorem 3.3 less than $1/4$ of the main term.

$$Er_1: \qquad p^{3n/2}|\mathscr{B}| < \frac{1}{4}\frac{|\mathscr{B}|^3}{p^3} \iff |\mathscr{B}| > 4p^{(3n/2)+3}. \tag{3.74}$$

$$Er_3: p^{(n/2)-2}|\mathscr{B}| \prod_{m_i \geq p} \frac{2m_i}{p} < \frac{1}{4}\frac{|\mathscr{B}|^2}{p^3} \iff |\mathscr{B}| > 4p^{(n/2)+1} \prod_{m_i \geq p} \frac{2m_i}{p}. \tag{3.75}$$

$$Er_5: \quad p^{n-2}|\mathscr{B}| \prod_{m_i \geq p^2} \frac{2m_i}{p^2} < \frac{1}{4}\frac{|\mathscr{B}|^2}{p^3} \iff |\mathscr{B}| > 4p^{n+1} \prod_{m_i \geq p^2} \frac{2m_i}{p^2}. \tag{3.76}$$

We may summarize the estimates (3.74), (3.75) and (3.76), in the form

Theorem 3.4. *Suppose that* $n \geq 4$ *is even, and that* $\Delta_p(Q) = -1$. *If* (3.74), (3.75) and (3.76), *hold, then*

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

In particular

$$\left|V \cap (\mathscr{B} + \mathscr{B})\right| \geq \frac{|\mathscr{B}|}{4p^3}.$$

As a corollary we obtain the existence of a primitive solution of the congruence in (3.1).

Corollary 3.4. *Under the hypotheses of Theorem* 3.4, $\mathscr{B} + \mathscr{B}$ *contains a primitive solution of* (3.1).

Proof. This is proved in exactly the same way as corollary 3.1. Indeed we have to prove

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

First of all, by Lemma 3.5, one can write

$$\sum_{\substack{\mathbf{x}\in V\\ p|\mathbf{x}}}\alpha(\mathbf{x}) = \sum_{\substack{p|x_i,\\ 1\le i\le n}}\alpha(\mathbf{x}) \overset{\text{by (3.37)}}{=} p^{2n}\sum_{y_i=1}^{p} a(p^2\mathbf{y}) \le |\mathscr{B}|\prod_{m_i\ge p}\frac{2m_i}{p} < \frac{|\mathscr{B}|^2}{4p^3}. \quad (3.77)$$

for all $n > 4$. Notice that the last inequality in (3.77) is possible in view of our hypothesis (3.75), which says

$$|\mathscr{B}| > 4p^{(n/2)+1}\prod_{m_i\ge p}\frac{2m_i}{p} \quad\Longleftrightarrow\quad \prod_{m_i\ge p}\frac{2m_i}{p} < \frac{|\mathscr{B}|}{4p^{(n/2)+1}}\,.$$

But by Theorem 3.4,

$$\sum_{\mathbf{x}\in V}\alpha(\mathbf{x}) \ge \frac{|\mathscr{B}|^2}{4p^3}\,,$$

It must therefore have

$$\sum_{\substack{\mathbf{x}\in V\\ p\nmid\mathbf{x}}}\alpha(\mathbf{x}) \ \ge \frac{|\mathscr{B}|^2}{4p^3} \ - \sum_{\substack{\mathbf{x}\in V\\ p|\mathbf{x}}}\alpha(\mathbf{x}) > 0\,,$$

finishing our proof. □

§3.6. Special case that $\mathscr{B}$ is cube $\mathscr{B}$, $\Delta = -1$.

Corollary 3.5. *Suppose* $n \ge 4$, $p > 2^{(2n+4)/(n-2)}$. *Let* $\mathscr{B}$ *be a cube centered at the origin with all* $m_i = B$, $B > 4^{1/n}p^{(3/2)+(3/n)}$. *Then* $\mathscr{B}+\mathscr{B}$ *contains a primitive solution of* (3.1).

Proof. We may assume $B = \left\lceil 4^{1/n}p^{(3/2)+(3/n)}\right\rceil$ and that $p > 2^{(2n+4)/(n-2)}$. Then trivially all the hypotheses of Corollary 3.4 are satisfied. Actually, for the hypothesis

$$(3.75) \iff B^n > 4p^{(n/2)+1}\prod_{m_i\ge p}\frac{2m_i}{p} = 4p^{(n/2)+1}\frac{2^nB^n}{p^n}$$
$$\iff p > 4^{2/(n-2)}2^{2n/(n-2)} = 2^{(2n+4)/(n-2)}.$$

Next for the condition (3.76), we designate two cases:

***Case* (i):** If $B > p^2$, we get

$$B^n > 4p^{n+1} \prod_{m_i \geq p^2} \frac{2m_i}{p^2} \iff B^n > 4p^{n+1} \frac{2^n B^n}{p^{2n}}$$
$$\iff p^{n-1} > 2^{n-2} \iff p > 2^{(n+2)/(n-1)}.$$

***Case* (ii):** If $B < p^2$, then (3.76) is

$$B^n > 4p^{n+1} \prod_{m_i \geq p^2} \frac{2m_i}{p^2} \iff B^n > 4p^{n+1}$$
$$\iff B > 4^{1/n} p^{1+(1/n)}.$$

Finally, for

$$(3.74) \iff B^n > 4p^{(3n/2)+3} \iff B > 4^{1/n} p^{(3/2)+(3/n)}.$$

Thus the hypotheses of Corollary 3.5 are satisfied and we obtain a primitive solution in the cube $\mathscr{B}$.□

§3.7. The main result.

Finally, we are in position to see

Theorem 3.5. *For any quadratic form $Q(\mathbf{x})$ with $n \geq 6$ and any prime p, there exists a primitive solution of* (3.1) *with*

$$\|\mathrm{x}\| \leq \begin{cases} \max\left\{2^7 p^{3/2}, 2^{38}\right\} & \text{for } \Delta = +1, \quad (3.78) \\ \max\left\{4^{2/n} p^{(3/2)+(3/n)}, 2^{(2n+4)/(n-2)}\right\} & \text{for } \Delta = -1. \quad (3.79) \end{cases}$$

Proof. Corollary 3.2 gives us (3.78) and Corollary 3.5 gives us (3.79).□

Chapter 4

Small Zeros of Quadratic Forms Modulo p^m

§4.1. Introduction.

Let $Q(\mathbf{x}) = Q(x_1, x_2, ..., x_n) = \sum_{1 \le i \le j \le n} a_{ij} x_i x_j$ be a quadratic form with integer coefficients and p be an odd prime. Suppose that n is even and $\det A_Q \not\equiv 0 \pmod{p}$, where A_Q is $n \times n$ defining matrix for $Q(\mathbf{x})$. Set $\|\mathbf{x}\| = \max|x_i|$ and let $V_{p^m} = V_{p^m}(Q)$ denote the set of zeros of Q in $\mathbb{Z}_{p^m}^n$. Let

$$\Delta_{p^m}(Q) = \begin{cases} \left((-1)^{n/2} \det A_Q \,/\, p\right) & \text{if} \quad p \nmid \det A_Q, \\ 0 & \text{if} \quad p \mid \det A_Q, \end{cases}$$

where $(\bullet / p)$ denotes the Legendre-Jacobi symbol and let $Q^*(\mathbf{x})$ be the inverse of the matrix representing $Q(\mathbf{x}), (\mathrm{mod}\, p^m)$. For $\mathbf{y} \in \mathbb{Z}_{p^m}^n$ set

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

where $e_{p^m}(x) = e^{2\pi i x / p^m}$.

The purpose of this chapter is to obtain small primitive solutions of the congruence,

$$Q(\mathbf{x}) \equiv 0 \pmod{p^m} \tag{4.1}$$

and more generally of obtaining primitive solution in a box $\mathscr{B}$ with $|\mathscr{B}|$

sufficiently large. As before we shall first calculate the Gauss sum

$$S = S(f, p^m) = \sum_{x=1}^{p^m} e_{p^m}\left(\lambda a\, x^2 + x\, y\ \right), \tag{4.2}$$

and then we apply this sum to calculate the function $\phi(V, \mathbf{y})$. Next we employ the calculation of $\phi(V, \mathbf{y})$ to obtain the fundamental identity. The problem of finding small primitive solution of (4.1) will reduce to a search for good bounds on the error terms of the fundamental identity. The final result of this chapter is stated in the following theorem.

Theorem 4.1. *For any quadratic form $Q(\mathbf{x})$ with n even, $n \geq 4$ and any odd prime power $p^m, m \geq 2$, there exists a primitive solution of* (4.1) *with* $\|\mathbf{x}\| \leq \max\{6^{1/n}\, p^{m[(1/2)+(1/n)]},\ 2^{2(n+1)/(n-2)} 3^{2/(n-2)}\}$.

We begin our work to prove this theorem.

§4.2. Determination of $\phi(V, \mathbf{y})$ modulo p^m.

We start this section by

4.2.1. Calculating the sum $S(f, p^m)$.

The following lemma allows us to find the evaluation of $\phi(V, \mathbf{y})$. A special case of this lemma (when $m = 2$) was proved in Chapter 2.

Lemma 4.1: *Let p be an odd prime with $p \nmid a$ and $\lambda, a \in \mathbb{Z}$. Let the sum S as in* (4.2). *Let $j \in \{0,1,2,\ldots,m-1\}$. Then*

$$S = \begin{cases} e_{p^{m-j}}(-\overline{4}\overline{a}\overline{\lambda'} y'^2) p^{(m+j)/2} & \text{if } p^j \| \lambda, p^j \,|\, y \text{ and } m-j \text{ is even}, \\ \chi(4a\lambda') e_{p^{m-j}}\left(-\overline{4}\overline{a}\overline{\lambda}' y'^2\right) G_p p^{(m+j-1)/2} & \text{if } p^j \| \lambda, p^j \,|\, y \text{ and } m-j \text{ is odd}, \\ 0 & \text{if } p^j \| \lambda, \text{but } p^j \nmid y, \end{cases}$$

where χ is the Legendre Symbol, $\lambda' = \lambda p^{-j}$, $y' = y p^{-j}$, and $\overline{\lambda}, \overline{\lambda}', \overline{a}$ are inverses $\bmod p^m$.

Proof. We shall prove Lemma 4.1 in the same fashion as the proof Lemma 2.1 of Chapter 2. We shall require applying Theorem 1.4 of

Chapter 1. Assume that $p \nmid a$. Then the critical point congruence is

$$p^{-t} f'(x) \equiv 0 \pmod{p}$$

or equivalently,

$$p^{-t}(\lambda a 2x + y) \equiv 0 \pmod{p}, \tag{4.3}$$

where $t = \mathrm{ord}_p(f')$. Now we have to treat two cases:

***Case* (i):** Assume that $p^j \| \lambda$ and $p^j | y$, with $j \in \{0,1,2,...,m-1\}$. Then $t = j$ because $p^t \| (2a\lambda, y)$. Thus (4.3) is equivalent to

$$2a \frac{\lambda}{p^j}\, x \equiv -\frac{y}{p^j} \pmod{p}. \tag{4.4}$$

Put $\lambda' = \lambda / p^j$ and $y' = y / p^j$, then (4.4) becomes

$$2a\lambda'\, x \equiv -y' \pmod{p}$$

or equivalently, there is a unique critical point α given by

$$\alpha = x \equiv -\overline{2a\lambda'} y' \pmod{p}.$$

Thus if $m - j$ is even,

$$S = S_\alpha = e_{p^m}\big(f(\alpha^*)\big) p^{(m+t)/2} = e_{p^m}\big(\lambda a \alpha^{*2} + y\alpha^*\big) p^{(m+j)/2},$$

where α^* is the unique lifting of α, to a solution of (4.3) $\bmod p^{(m-j+1)/2}$. We can take $\alpha^* \equiv -\overline{2}\,\overline{a}\,\overline{\lambda'}\, y' \pmod{p^m}$ where $\overline{a}, \overline{\lambda}$ are inverses $\bmod p^m$. Then

$$\begin{aligned} f(\alpha^*) = \lambda a \alpha^{*2} + y\alpha^* &\equiv p^j \lambda' a \overline{\lambda'}^2 \overline{4}\,\overline{a}^2 y'^2 - p^j y'^2 \overline{\lambda'} \overline{2a} \pmod{p^m} \\ &\equiv p^j y'^2 (\overline{4}\,\overline{a}\,\overline{\lambda'} - \overline{2}\,\overline{a}\,\overline{\lambda'}) \pmod{p^m} \\ &\equiv -\overline{4}\,\overline{a}\,\overline{\lambda'} y'^2 p^j \pmod{p^m} \end{aligned}$$

and so $S_\alpha = e_{p^{m-j}}(-\overline{4}\,\overline{a}\,\overline{\lambda'} y'^2) p^{(m+j)/2}$.

If $m - j$ is odd, then

$$A_\alpha \equiv 2p^{-t} f''(\alpha^*) \equiv 2p^{-j} 2a\lambda \equiv 4a\lambda' \pmod{p}.$$

Thus

$$\begin{aligned} S = S_\alpha &= \chi_2(A_\alpha)\, e_{p^m}(\lambda a \alpha^{*2} + y\alpha^*) G_p p^{(m+j-1)/2} \\ &= \chi_2(4a\lambda')\, e_{p^{m-j}}(-\overline{4}\,\overline{a}\,\overline{\lambda'} y'^2) G_p p^{(m+j-1)/2}. \end{aligned}$$

***Case* (ii):** Suppose that $p^j \| \lambda$ but $p^j \nmid y$, with $j \in \{1,2,...,m-1\}$; say

$p^k \| y$ with $k < j$. Then we see that $t = k$. By (3.1), the critical point congruence is

$$p^t (2a\lambda x) \equiv -yp^{-t} \pmod{p},$$

or equivalently

$$0 \equiv -yp^k \pmod{p},$$

which has no solution. Consequently $S = 0$, and this completes the proof of Lemma 4.1. □

4.2.2. Evaluating $\phi(V, \mathbf{y})$ for the case of a diagonal quadratic form.

Suppose that $Q(\mathbf{x}) = \sum_{i=1}^{n} a_i x_i^2$; with $p \nmid a_i$, $1 \le i \le n$. We remark that if $\mathbf{y} \neq \mathbf{0}$, then by the orthogonality property of exponential sums,

$$\begin{aligned}\sum_{\mathbf{x}\in\mathbf{V}} e_{p^m}(\mathbf{x}\cdot\mathbf{y}) &= \sum_{\mathbf{x}\in\mathbb{Z}_{p^m}^n} p^{-m}\Bigg(\sum_{\lambda=0}^{p^m-1} e_{p^m}\left(\lambda Q(\mathbf{x})\right)\Bigg) e_{p^m}(\mathbf{x}\cdot\mathbf{y}) \\ &= p^{-m}\sum_{\lambda}\sum_{\mathbf{x}} e_{p^m}(\lambda Q(\mathbf{x}) + \mathbf{x}\cdot\mathbf{y}) \\ &= \underbrace{p^{-m}\sum_{\mathbf{x}} e_{p^m}(\mathbf{x}\cdot\mathbf{y})}_{S_1} + \underbrace{p^{-m}\sum_{\lambda\neq 0}\sum_{\mathbf{x}} e_{p^m}(\lambda Q(\mathbf{x}) + \mathbf{x}\cdot\mathbf{y})}_{S_2}.\end{aligned}$$

Now, if $\mathbf{y} = \mathbf{0}$, this implies that

$$|V| = p^{m(n-1)} + S_2 \quad \Rightarrow \quad S_2 = |V| - p^{m(n-1)} = \phi(V, \mathbf{0}).$$

Next suppose that $\mathbf{y} \neq \mathbf{0}$. Then, by (1.19) of Chapter 1, as some $y_i \neq 0$,

$$S_1 = p^{-m}\sum_{\mathbf{x}} e_{p^m}(\mathbf{x}\cdot\mathbf{y}) = p^{-m}\prod_{i=1}^{n}\sum_{x_i}^{p^m} e_{p^m}(x_i y_i) = 0,$$

while

$$\begin{aligned}S_2 &= p^{-m}\sum_{\lambda\neq 0}\sum_{\mathbf{x}} e_{p^m}(\lambda Q(\mathbf{x}) + \mathbf{x}\cdot\mathbf{y}) \\ &= p^{-m}\sum_{\lambda\neq 0}\underbrace{\sum_{\mathbf{x}} e_{p^m}\left(\lambda(a_1x_1^2 + a_2x_2^2 + \cdots + a_nx_n^2) + x_1y_1 + x_2y_2 + \cdots + x_ny_n\right)}_{S_\lambda}.\end{aligned} \tag{4.5}$$

Hence we have $S_2 = \phi(V, \mathbf{y})$ for all $\mathbf{y}$. From now on we shall use $\phi(V, \mathbf{y})$

to mean S_2 and vice versa. We shall treat the inside sum S_λ in (4.5) separately.

4.2.3. The sum S_λ.

The sum S_λ in (4.5) may be rewritten

$$\begin{aligned} S_\lambda &= \sum_{\mathbf{x}} e_{p^m}\left([\lambda a_1 x_1^2 + x_1 y_1] + \cdots + [\lambda a_n x_n^2 + y_n x_n]\right) \\ &= \sum_{x_1} e_{p^m}(\lambda a_1 x_1^2 + y_1 x_1) \cdots \sum_{x_n} e_{p^m}(\lambda a_n x_n^2 + y_n x_n) \qquad (4.6) \\ &= \prod_{i=1}^{n} \underbrace{\sum_{x_i=1}^{p^m} e_{p^m}(\lambda a_i x_1^2 + x_i y_i)}_{\text{Gauss sum}}. \end{aligned}$$

We have the following analogue of Lemma 2.2 of Chapter 2.

Lemma 4.2: *Suppose n is even. Let S_λ as in (4.6). Let $p^j \| \lambda$, $0 \le j \le m-1$. Assume $p \nmid a_1 \cdot a_2 \cdot \cdots \cdot a_n$. Then*

$$S_\lambda = \begin{cases} \delta_j p^{(m+j)n/2} e_{p^{m-j}}(-\overline{4}\overline{\lambda'} Q^*(\mathbf{y}')) & \text{if } p^j \,|\, y_i, \text{ for all } i, \\ 0 & \text{if } p^j \nmid y_i, \text{ for some } i, \end{cases} \qquad (4.7)$$

where $\lambda' = p^{-j}\lambda, y' = p^{-j}y$ and

$$\delta_j = \begin{cases} 1 & \text{if } m-j \text{ is even}, \\ \Delta & \text{if } m-j \text{ is odd}. \end{cases} \qquad (4.8)$$

with $\Delta = \chi\left((-1)^{n/2}\right)\chi(a_1 \cdots a_n)$, $\chi = \chi_2$.

Proof. First let us suppose that $p^j \| \lambda$ and that $p^j | y_i$ for all i. Put $\lambda' = p^{-j}\lambda$ *and* $y_i' = p^{-j} y_i$. Then by Lemma 4.1, if $m-j$ is even,

$$\begin{aligned} S_\lambda &= e_{p^{m-j}}(-\overline{4}\overline{a_1}\overline{\lambda'}\, y_1'^2) p^{(m+j)/2} \cdots e_{p^{m-j}}(-\overline{4}\overline{a_n}\overline{\lambda'}\, y_n'^2) p^{(m+j)/2} \\ &= p^{(m+j)n/2} e_{p^{m-j}}\Big((-\overline{4})\overline{a_1}\,\overline{\lambda'}\, y_1'^2 + (-\overline{4})\overline{a_2}\overline{\lambda'}\, y_2'^2 + \cdots + (-\overline{4})\overline{a_n}\,\overline{\lambda'}\, y_n'^2\Big) \\ &= p^{(m+j)n/2} e_{p^{m-j}} \underbrace{\Big(\Big((-\overline{4})\,\overline{\lambda'}\Big)\Big(\overline{a_1} y_1'^2 + \overline{a_2} y_2'^2 + \cdots + \overline{a_n}\, y_n'^2\Big)\Big)}_{-\overline{4}\overline{\lambda} Q^*(y_1,\ldots,y_n) = \overline{-4\lambda} Q^*(\mathbf{y}),} \\ &= p^{(m+j)n/2} e_{p^{m-j}}\left(-\overline{4}\overline{\lambda'} Q^*(\mathbf{y}')\right), \end{aligned}$$

where $Q^*(\mathbf{y})$, as defined earlier, is the quadratic form associated with

the inverse of the matrix for $Q \bmod p^m$. If $m-j$ is odd, then again by Lemma 4.1,

$$\begin{aligned}
S_\lambda &= \chi(4a_1\lambda')\, e_{p^{m-j}}(-\overline{4}\overline{a}_1\overline{\lambda}' y_1'^2) G_p p^{(m+j-1)/2} \cdot \cdots \\
&\qquad \cdot \chi(4a_1\lambda')\, e_{p^{m-j}}(-\overline{4}\overline{a}_n\overline{\lambda}' y_n'^2) G_p p^{(m+j-1)/2} \\
&= p^{n(m+j-1)/2} G_p^n\, \chi(4\lambda' a_1 \cdots 4\lambda' a_n)\, e_{p^{m-j}}\Big(\overline{(-4)}\ \overline{\lambda}' Q^*(y_1'^2 + y_2'^2 + \cdots + y_n'^2)\Big) \\
&= p^{n(m+j-1)/2} p^{n/2} \overbrace{\chi\Big((-1)^{n/2}\Big)\ \underbrace{\chi(a_1 \cdots a_n)}_{n \text{ is even}}}^{\Delta}\ e_{p^{m-j}}\Big(\overline{(-4)}\ \overline{\lambda}'\ Q^*(\mathbf{y}')\Big) \\
&= p^{n(m+j)/2} \Delta\, e_{p^{m-j}}\Big(\overline{(-4)}\ \overline{\lambda}'\ Q^*(\mathbf{y}')\Big).
\end{aligned}$$

Next suppose that $p^j \| \lambda$ but $p^j \nmid y_i$ for some i. Then it is easily seen that (by Lemma 4.1) $S_\lambda = 0$. Thus the proof of Lemma 4.2 is complete. □

Following the same method as in subsection 2.2.5 of Chapter 2, this Lemma can be generalized to an arbitrary nonsingular quadratic form (mod p^m) as follows.

Lemma 4.3: *Let p be an odd prime, n be even and $Q(\mathbf{x})$ any quadratic form. Let $p^j \| \lambda$, $0 \le j \le m-1$. Assume $\det A_Q \not\equiv 0 (\bmod p)$, where A_Q is the $n \times n$ defining matrix for $Q(\mathbf{x})$. Then*

$$S_\lambda = \begin{cases} \delta_j p^{(m+j)n/2} e_{p^{m-j}}(-\overline{4}\overline{\lambda'} Q^*(\mathbf{y}')) & \text{if } p^j \,|\, y_i, \text{ for all } i, \\ 0 & \text{if } p^j \nmid y_i, \text{ for some } i, \end{cases}$$

where $\lambda' = p^{-j}\lambda, y' = p^{-j}y$ and as given in (4.8).

4.2.4. Formula for $\phi(V, \mathbf{y})$.

We are now ready to prove

Lemma 4.4. *Let n be an even positive integer. Then*

$$\phi(V, \mathbf{y}) = p^{mn/2-m} \sum_{\substack{j=0 \\ p^j | y_i \text{ for all } i}}^{m-1} \delta_j p^{jn/2} \omega_j(\mathbf{y}'),$$

where $\mathbf{y}' = p^{-j}\mathbf{y}$, δ_j as defined in (4.8) and

$$\omega_j(\mathbf{y}') = \begin{cases} p^{m-j} - p^{m-j-1} & , \quad p^{m-j} \,|\, Q^*(\mathbf{y}'), \\ -p^{m-j-1} & , \quad p^{m-j-1} \,\|\, Q^*(\mathbf{y}'), \\ 0 & , \quad p^{m-j-1} \nmid Q^*(\mathbf{y}'). \end{cases}$$

Proof. Recall from subsection 4.2.2 that $\phi(V,\mathbf{y}) = p^{-m}\sum_{\lambda \neq 0} S_\lambda = S_2$. Fix $\mathbf{y} = (y_1,...,y_n)$. Put $\mathbf{y}' = p^{-j}\mathbf{y}$, $\lambda' = p^{-j}\lambda$. Then according to Lemma 4.3,

$$\begin{aligned} \sum_{\lambda=1}^{p^m-1} S_\lambda &= \sum_{\substack{j=0 \\ p^j | y_i, \text{ for all } i}}^{m-1} \sum_{\substack{\lambda \\ p^j \| \lambda}} \delta_j p^{(m+j)n/2} e_{p^{m-j}}\left(-\overline{4}\overline{\lambda}' Q^*(\mathbf{y}')\right) \\ &= \sum_{\substack{j=0 \\ p^j | y_i, \text{ for all } i}}^{m-1} \delta_j p^{(m+j)n/2} \sum_{\substack{\lambda'=1 \\ p \nmid \lambda'}}^{p^{m-j}} e_{p^{m-j}}\left(-\overline{4}\overline{\lambda}' Q^*(\mathbf{y}')\right) \\ &= \sum_{\substack{j=0 \\ p^j | y_i, \text{ for all } i}}^{m-1} \delta_j p^{(m+j)n/2}\ \omega_j(\mathbf{y}'), \end{aligned}$$

where we have used Lemma 1.5 of Chapter 1 applied to the second sum in the second step above. Hence, it follows that

$$\phi(V,\mathbf{y}) = p^{-m} \sum_{\substack{j=0 \\ p^j | y_i, \text{ for all } i}}^{m-1} \delta_j p^{(m+j)n/2}\ \omega_j(\mathbf{y}') = p^{mn/2-m} \sum_{\substack{j=0 \\ p^j | y_i \text{ for all } i}}^{m-1} \delta_j p^{jn/2} \omega_j(\mathbf{y}').$$

This completes the proof of Lemma 4.4. □

§4.3. Small solutions of the quadratic congruence $Q(\mathbf{x}) \equiv 0 \pmod{p^m}$.

In this section we derive the fundamental identity $\bmod p^m$ (the general case). Then we use it to find small primitive solutions of the quadratic congruence (4.1).

4.3.1. The fundamental identity.

Let V_{p^m} be as we defined above. Let $\alpha(\mathbf{x})$ be a real function defined on $\mathbb{Z}_{p^m}^n$ with finite Fourier expansion $\alpha(\mathbf{x}) = \sum_{\mathbf{y}} a(\mathbf{y}) e_{p^m}(\mathbf{x}\cdot\mathbf{y})$, where $a(\mathbf{y}) = p^{-mn}\sum_{\mathbf{x}} \alpha(\mathbf{x}) e_{p^m}(-\mathbf{x}\cdot\mathbf{y})$. Then by definition of $\phi(V,\mathbf{y})$,

$$\begin{aligned}\sum_{\mathbf{x}\in V_{p^m}}\alpha(\mathbf{x}) &= a(\mathbf{0})\big|V_{p^m}\big| + \sum_{\mathbf{y}\neq\mathbf{0}} a(\mathbf{y}) \sum_{\mathbf{x}\in V_{p^m}} e_{p^m}(\mathbf{y}\cdot\mathbf{x}) \\ &= a(\mathbf{0})\big|V_{p^m}\big| + \sum_{\mathbf{y}\neq\mathbf{0}} a(\mathbf{y})\,\phi(V,\mathbf{y}) \\ &= a(\mathbf{0})\big[\phi(V,\mathbf{0}) + p^{m(n-1)}\big] + \sum_{\mathbf{y}\neq\mathbf{0}} a(\mathbf{y})\,\phi(V,\mathbf{y}) \\ &= a(\mathbf{0})p^{m(n-1)} + \sum_{\mathbf{y}} a(\mathbf{y})\,\phi(V,\mathbf{y}) \\ &= p^{-mn}\sum_{\mathbf{x}}\alpha(\mathbf{x})p^{m(n-1)} + \sum_{\mathbf{y}} a(\mathbf{y})\,\phi(V,\mathbf{y}).\end{aligned}$$

Thus by Lemma 4.4,

$$\begin{aligned}\sum_{\mathbf{x}\in V_{p^m}}\alpha(\mathbf{x}) &= p^{-m}\sum_{\mathbf{x}}\alpha(\mathbf{x}) + p^{mn/2-m}\sum_{\mathbf{y}} a(\mathbf{y}) \sum_{\substack{j=0 \\ p^j|y_i \text{ for all } i}}^{m-1} \delta_j p^{jn/2}\omega_j(\mathbf{y}') \\ &= p^{-m}\sum_{\mathbf{x}}\alpha(\mathbf{x}) + p^{mn/2-m} \sum_{j=0}^{m-1} \delta_j p^{jn/2} \sum_{\substack{\mathbf{y} \\ p^j|y_i \text{ for all } i}} a(\mathbf{y})\,\omega_j(\mathbf{y}').\end{aligned}$$

But by noticing that the inner sum $\sum_{\mathbf{y}} a(p^j\mathbf{y}')\,\omega_j(y')$ can be written

$$\begin{aligned}\sum_{\substack{\mathbf{y} \\ p^j|y_i \text{ for all } i}} a(\mathbf{y})\,\omega_j(\mathbf{y}') &= \sum_{y'(\mathrm{mod}\, p^{m-j})} a(p^j\mathbf{y}')\;\omega_j(\mathbf{y}') \\ &= \sum_{\substack{\mathbf{y}' \\ p^{m-j}|Q^*(\mathbf{y}')}} a(p^j\mathbf{y}')\big(p^{m-j}-p^{m-j-1}\big) - \sum_{\substack{\mathbf{y}' \\ p^{m-j-1}\|Q^*(\mathbf{y}')}} a(p^j\mathbf{y}')p^{m-j-1} \\ &= \sum_{\substack{\mathbf{y}' \\ p^{m-j}|Q^*(\mathbf{y}')}} a(p^j\mathbf{y}')\,p^{m-j} - p^{m-j-1} \sum_{\substack{\mathbf{y}' \\ p^{m-j-1}|Q^*(\mathbf{y}')}} a(p^j\mathbf{y}'),\end{aligned}$$

we obtain,

Theorem 4.2. [The fundamental identity] *For any* $\alpha(\mathbf{x})$ *as given above*

$$\begin{aligned}\sum_{\mathbf{x}\in V_{p^m}}\alpha(\mathbf{x}) &= p^{-m}\sum_{\mathbf{x}\,(\mathrm{mod}\,p^m)}\alpha(\mathbf{x}) \\ &\quad + p^{mn/2}\sum_{j=0}^{m-1} p^{jn/2}\delta_j\Bigg(p^{-j}\sum_{\substack{y_i'=1 \\ p^{m-j}|Q^*(\mathbf{y}')}}^{p^{m-j}} a(p^j\mathbf{y}') - p^{-j-1}\sum_{\substack{y_i'=1 \\ p^{m-j-1}|Q^*(\mathbf{y}')}}^{p^{m-j}} a(p^j\mathbf{y}')\Bigg).\end{aligned} \tag{4.9}$$

where δ_j *as we defined in* (4.8): $\delta_j = 1$ when $m-j$ is even and $\delta_j = \Delta$ if $m-j$ is odd.

4.3.2. Auxiliary lemma on estimating the sum $\sum_{y_i=1}^{p^{m-j}} a(p^j\mathbf{y})$.

Let $\mathscr{B}$ be a box centered at the origin defined by

$$\mathscr{B} = \left\{\mathbf{x} \in \mathbb{Z}^n \,\middle|\, a_i \le x_i < a_i + B_i, 1 \le i \le n\right\}, \tag{4.10}$$

where $a_i, B_i \in \mathbb{Z}$ and $1 \le B_i \le p^m$, $1 \le i \le n$. Then $|\mathscr{B}| = \prod_{i=1}^n B_i$, the cardinality of $\mathscr{B}$. View the box $\mathscr{B}$ in (4.10) as a subset of $\mathbb{Z}_{p^m}^n$ and let $\alpha(\mathbf{x}) = \chi_{\mathscr{B}} * \chi_{\mathscr{B}}$ with Fourier expansion $\alpha(\mathbf{y}) = \sum_{\mathbf{y}} a(\mathbf{y}) e_{p^m}(\mathbf{x}\cdot\mathbf{y})$. Thus for any $\mathbf{y} \in \mathbb{Z}_{p^m}^n$,

$$\left|a(\mathbf{y})\right| = p^{-mn} \prod_{i=1}^n \left|\frac{\sin^2 \pi B_i y_i / p^m}{\sin^2 \pi y_i / p^m}\right|,$$

where the term in the product is taken to be m_i if $y_i = 0$. In particular

$$a(\mathbf{y}) \le p^{-mn} \prod_{i=1}^n \min\left\{B_i^2, \left(\frac{p^m}{2y_i}\right)^2\right\}. \tag{4.11}$$

Consider the congruence (4.1):

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

where $Q(\mathbf{x})$ is a quadratic form. Our task in the next section is bounding the error terms in the fundamental identity (4.9); see Theorem 4.2. But to do this we need to develop a general lemma similar to the Lemmas 2.8 (Chapter 2) and 3.4, 3.5 (Chapter 3).

Lemma 4.5. Let $\mathscr{B}$ be any box of type (4.10) and $\alpha(\mathbf{x}) = \chi_{\mathscr{B}} * \chi_{\mathscr{B}}(\mathbf{x})$. Then we have

$$\sum_{y_i=1}^{p^{m-j}} a(p^j\mathbf{y}) \le \frac{|\mathscr{B}|}{p^{jn}} \prod_{B_i \ge p^{m-j}} \frac{2B_i}{p^{m-j}}.$$

Proof. First,

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

$$= \sum_{\substack{x_i=1 \\ \mathbf{x} \equiv \mathbf{0} \,(\mathrm{mod}\, p^{m-j})}}^{p^m} p^{-mn}\alpha(\mathbf{x})p^{(m-j)n}$$

$$= p^{-jn} \sum_{\substack{x_i=1 \\ \mathbf{x} \equiv \mathbf{0} \,(\mathrm{mod}\, p^{m-j})}}^{p^m} \alpha(\mathbf{x})$$

$$= p^{-jn} \sum_{\substack{\mathbf{u}\in\mathscr{B} \\ \mathbf{u}+\mathbf{v} \equiv 0 \,(\mathrm{mod}\, p^{m-j})}} \sum_{\mathbf{v}\in\mathscr{B}} 1$$

$$\leq p^{-jn} \prod_{i=1}^{n} B_i \left(\left[\frac{B_i}{p^{m-j}} \right] + 1 \right). \tag{4.12}$$

To verify the last inequality in (4.12) we count the number of solutions of the congruence

$$\mathbf{u} + \mathbf{v} \equiv 0 \pmod{p^{m-j}},$$

with $\mathbf{u}, \mathbf{v} \in \mathscr{B}$. Actually for each choice of $\mathbf{v}$, there are at most $\prod_{i=1}^{n}([B_i / p^{m-j}]+1)$ choices $\mathbf{u}$. Thus the total number of solutions is less than or equal to $\prod_{i=1}^{n}([B_i / p^{m-j}]+1)$. Hence it follows from (4.12),

$$\sum_{y_i=1}^{p^2} a(p\mathbf{y}) \leq p^{-jn} \prod_{i=1}^{n} B_i \left(\left[\frac{B_i}{p^{m-j}} \right] + 1 \right). \tag{4.13}$$

We may split the product in (4.13) such that

$$\prod_{i=1}^{n} B_i \left(\left[\frac{B_i}{p^{m-j}} \right] + 1 \right) = \prod_{B_i < p^{m-j}} B_i \prod_{B_i \geq p^{m-j}} B_i \left(\frac{2B_i}{p^{m-j}} \right).$$

Then by this equality we therefore have

$$\sum_{y_i=1}^{p^{m-j}} a(p^j\mathbf{y}) \leq \frac{|\mathscr{B}|}{p^{jn}} \prod_{B_i \geq p^{m-j}} \frac{2B_i}{p^{m-j}}.$$

Our proof is complete. □

4.3.3. Bounds on the error terms of the fundamental identity (mod p^m) for the case of cube $\mathscr{B}$.

The error term in the fundamental identity is given by

$$Error = p^{mn/2} \sum_{j=0}^{m-1} p^{jn/2} \delta_j \left(p^{-j} \sum_{\substack{y'_i=1 \\ p^{m-j} \mid Q^*(\mathbf{y}')}}^{p^{m-j}} a(p^j\mathbf{y}') - p^{-j-1} \sum_{\substack{y'_i=1 \\ p^{m-j-1} \mid Q^*(\mathbf{y}')}}^{p^{m-j}} a(p^j\mathbf{y}') \right).$$

By Lemma 4.5 we get

$$|Error| \le p^{mn/2} \sum_{j=0}^{m-1} p^{jn/2} \left| \sum_{y_i=1}^{p^{m-j}} \varphi(\mathbf{y})\ a(p^j \mathbf{y}') \right|, \tag{4.14}$$

where

$$\varphi(\mathbf{y}) = \begin{cases} p^j - p^{-j-1} & \text{if} \quad p^{m-j} \,|Q^*(\mathbf{y}), \\ -p^{-j-1} & \text{if} \ \ p^{m-j-1} \,\|Q^*(\mathbf{y}). \end{cases}$$

Continuing from (4.14),

$$\begin{aligned} |Error| &\le p^{mn/2} \sum_{j=0}^{m-1} p^{(jn/2)-j} \frac{|\mathscr{B}|}{p^{jn}} \prod_{B_i \ge p^{m-j}} \frac{2B_i}{p^{m-j}} \\ &= p^{mn/2}\, |\mathscr{B}| \sum_{j=0}^{m-1} \frac{1}{p^{(jn/2)+j}} \prod_{B_i \ge p^{m-j}} \frac{2B_i}{p^{m-j}}. \end{aligned} \tag{4.15}$$

We now restrict our attention to the case where $\mathscr{B}$ is cube, that is, $B_i = B\,,\ 1 \le i \le n\,.$ Say $p^{j_0} \le B < p^{j_0+1}$ for some $j_0 \in \mathbb{N}, 1 \le j_0 < m\,.$ Then

$$B \ge p^{m-j} \quad \Longleftrightarrow \quad m - j \le j_0 \quad \Longleftrightarrow \quad j \ge m - j_0.$$

Continuing from (4.15), we get

$$\begin{aligned} |Error| &\le p^{mn/2}\, |\mathscr{B}| \sum_{j=m-j_0}^{m-1} \frac{2^n\, |\mathscr{B}|}{p^{(jn/2)+j} p^{nm-nj}} + p^{mn/2}\, |\mathscr{B}| \sum_{j=0}^{m-j_0-1} \frac{1}{p^{(jn/2)+j}} \\ &= \frac{2^n\, |\mathscr{B}|^2}{p^{mn/2}} \sum_{j=m-j_0}^{m-1} p^{(n/2)j-j} + p^{mn/2}\, |\mathscr{B}| \sum_{j=0}^{m-j_0-1} \frac{1}{p^{(jn/2)+j}} \\ &< \frac{2^n\, |\mathscr{B}|^2}{p^{mn/2}}\, p^{[(n/2)-1](m-1)} \cdot 2 + p^{mn/2}\, |\mathscr{B}| \cdot 2 \\ &= 2^{n+1}\, |\mathscr{B}|^2\ p^{-m-(n/2)+1} + 2p^{mn/2}\, |\mathscr{B}| \\ &= \frac{2^{n+1}\, |\mathscr{B}|^2}{p^{m+(n/2)-1}} + 2p^{mn/2}\, |\mathscr{B}|. \end{aligned}$$

4.3.4. The main results.

Theorem 4.3. *Suppose that $m \ge 2,\ n \ge 4\,,\ n$ even. Then for any cube $\mathscr{B}$ centered at the origin,*

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

where

$$|Error| \le \underbrace{\frac{2^{n+1}\,|\mathscr{B}|^2}{p^{m+(n/2)-1}}}_{Error\,1} + \underbrace{2p^{mn/2}\,|\mathscr{B}|}_{Error\,2}.$$

We compare *Error* 1 and *Error* 2 in Theorem 4.3 to the main term $|\mathscr{B}|^2 / p^m$. In order to make the left-hand side positive, we make each error term less than 1/3 of the main term. For the error term *Error* 1, we need

$$\frac{2^{n+1}\,|\mathscr{B}|^2}{p^{m+(n/2)-1}} < \frac{1}{3}\frac{|\mathscr{B}|^2}{p^m} \quad \Longleftrightarrow \quad p^{(n/2)-1} > 3.2^{n+1}$$
$$\Longleftrightarrow \quad p > 2^{2(n+1)/(n-2)} \cdot 3^{2/(n-2)}. \tag{4.16}$$

For the error term *Error* 2,

$$2p^{mn/2}\,|\mathscr{B}| < \frac{1}{3}\frac{|\mathscr{B}|^2}{p^m} \quad \Longleftrightarrow \quad |\mathscr{B}| > 3.2\ p^{(mn/2)+m}$$
$$\Longleftrightarrow \quad B > 6^{1/n}\,p^{(m/2)+(m/n)}. \tag{4.17}$$

Collecting together the two criteria (4.16) and (4.17), we obtain

Theorem 4.4. *Suppose that* $m \ge 2$, $n \ge 4$, n *even. Then for any cube* $\mathscr{B}$ *centered at the origin, if* (4.16), (4.17) *hold, then*

$$\sum_{\mathbf{x}\in V} \alpha(\mathbf{x}) \ge \frac{1}{3}\frac{|\mathscr{B}|^2}{p^m}.$$

In particular

$$\left|V \cap (\mathscr{B} + \mathscr{B})\right| \ge \frac{|\mathscr{B}|}{3p^m}.$$

It remains to prove under the hypothesis of Theorem 4.4, the existence of primitive solutions of the congruence (4.1). Recall $\mathbf{x}$ is called primitive if $\gcd(x_1,\ldots,x_n,p) = 1$. We shall write $p|\mathbf{x}$ for imprimitive points. Thus we have to prove

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

Corollary 4.1. *Suppose* $m \ge 2$, $n > m$, n *even* $p > 2^{2(n+1)/(n-2)}3^{2/(n-2)}$ *and* $\mathscr{B}$ *is a cube with* $B > 6^{1/n}\,p^{(m/2)+(m/n)}$. *Then* $\mathscr{B} + \mathscr{B}$ *contains a*

primitive solution of (4.1).

Proof. As in the proof of Lemma 4.5 with $j = m-1$, we have

$$\begin{aligned}\sum_{\substack{\mathbf{x}\in V\\ p|\mathbf{x}}}\alpha(\mathbf{x}) = \sum_{\substack{p|x_i,\\ 1\le i\le n}}\alpha(\mathbf{x}) &< \sum_{\substack{\mathbf{u}\in\mathscr{B}\\ \mathbf{u}+\mathbf{v}\,\equiv\,0\,(\mathrm{mod}\,p)}}\sum_{\mathbf{v}\in\mathscr{B}}1\\ &\le \prod_{i=1}^{n}B_i\left(\left[\frac{B_i}{p}\right]+1\right)\\ &= B^n\left(\left[\frac{B_i}{p}\right]+1\right)^n\\ &< \frac{B^{2n}}{p^n}\left(1+\frac{p}{B}\right)^n\\ &\le \frac{B^{2n}}{p^n}(1+\varepsilon)^n,\end{aligned}$$

where $\varepsilon < p^{-[(m/2)+(m/n)]+1}$. However according to Theorem 4.4 we have,

$$\sum_{\mathbf{x}\in V}\alpha(\mathbf{x}) \ge \frac{|\mathscr{B}|^2}{3p^m}.$$

Hence it follows that

$$\begin{aligned}\sum_{\substack{\mathbf{x}\in V\\ p\nmid\mathbf{x}}}\alpha(\mathbf{x}) &\ge \frac{|\mathscr{B}|^2}{3p^m} - \sum_{\substack{\mathbf{x}\in V\\ p|\mathbf{x}}}\alpha(\mathbf{x})\\ &\ge \frac{|\mathscr{B}|^2}{3p^m} - \frac{B^{2n}}{p^n}(1+\varepsilon)^n > 0,\end{aligned}$$

by our hypotheses on the size of p. This completes the proof. □

We close this chapter with

***Proof of Theorem* 4.1.** It follows directly from Corollary 4.1.□

Bibliography

[**1**] T. Cochrane, *Small solutions of conguences.* PhD thesis, University of Michigan, 1984

[**2**] _____, *The distribution of solutions to equations over finite fields*, American Mathematical Society, Vol. 293 No. 2 (1986), 819-826

[**3**] _____, *On a trigonometric inequality of Vinogradov,* J. Number Theory 27 (1987), 9-16.

[**4**] _____, *Small solutions of congruences over algebraic number fields*, Illinois J.Math 31 (1987), 618-625.

[**5**] _____, *Small zeros of quadratic forms modulo p*, J. Number Theory 33, No. 3 (1989), 286-292.

[**6**] _____, *Small zeros of quadratic forms modulo p*, II, Proceedings of the Illinois Number Theory Conference, (1989), Birkhauser, Boston (1990), 91-94

[**7**] _____, *Small zeros of quadratic congruences modulo pq*, Mathematika 37 (1990), No. 2, 261-272.

[**8**] _____, *Small zeros of quadratic forms modulo p*, III, Number Theory 33, No. 1 (1991), 92-99.

[**9**] _____, *On representing the multiple of a number by a quadratic form*, Acta Arithmetica, LXIII. 3 (1993).

[**10**] _____, *Small zeros of quadratic congruences modulo pq,* II, Number Theory 50 (1995), No. 2, 299-308.

[**11**] _____ and Z. Zheng, *Pure and mixed exponential s*ums, *Acta Arithmetica*, XCI.3. (1999), 249-278.

[**12**] _____ and J.C.Peral, *An asymptotic formula for a trigonometric sum of Vinogradov,* J. Number Theory 91 (2001),1-19.

[**13**] L. Carlitz, *Weighted quadratic partitions over a finite field*, Canad. J. Math. 5 (1953), 317-323.

[**14**] _____, *Weighted quadratic partitions* $(\mathrm{mod}\, p^r)$, Math Zeitschr. Bd. 59, (1953), 40-46

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

[**16**] _____, *Small solutions of quadratic congruences* II, Mathematica, 38 (1991), 264-284.

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

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

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

[**20**] _____, *Small solutions of congruences.* J. Number Theory 45 (1993), No. 3, 261-280.

[**21**] _____, *On small zeros of quadratic forms over finite fields.* (II), Acta Mathematica Sinica, New Series 1993, Vol. 9, No. 4, 382-389 .

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

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

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

[25] G. L. Watson, *Integral Quadratic Forms*, Cambridge University Press, 1960.

[26]. *International Conference on Integral Forms and Lattices, Integral quadratic forms and lattices,* Proceedings of the International Conference on Integral Quadratic Forms and lattices, Jun 15-19, 1998, Seoul National University, Korea/ Myung-Hwan Kim...[et al.].

[27] Z. I. Borevich and I.R.Shafarevich, *Number Theory*, Academic Press, 1966.

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

[29] R. Lidl and H. Niederreiter, *Encyclopedia of Mathematics and its Applications, Finite Fields*, Addison-Wesley Publishing Company, 1983.