Counting lattice points of quadratic forms over the ring $\mathbb{Z}_{p^3}$

Ali H. Hakami
Department of Mathematics
Science Faculty of Jazan University

Let $Q(x) = Q(x_1, x_2, \ldots, x_n)$ be a quadratic form in $n$-variables with integer coefficients. We obtain bounds on the lattice points over the ring $\mathbb{Z}_{p^3}$ to the congruence $Q(x) \equiv 0 \pmod{p^3}$ in a general rectangular box. We use Fourier series and exponential sums to obtain our results.

Introduction

Let $Q(x) = Q(x_1, x_2, \ldots, x_n) = \sum a_{ij} x_i x_j$ be a nonsingular quadratic form with integer coefficients in $n$-variables. Let $V_{p^3} \cap = \sum a_{ij} x_i x_j$ be a nonsingular quadratic form in $n$-variables. Let $V_{p^3}$ be the set of integral solutions of the equation defined by

$$Q(x) \equiv 0 \pmod{p^3}, \quad (1)$$

where $(\cdot/p)$ denotes the Legendre-Jacobi symbol. In this paper we shall use Fourier series and exponential sums to find points in $V$ with the variables restricted to the box $B$ of the type (2), so that $V \cap B$ is nonempty and determine the cardinality $|V \cap B|$ of $V \cap B$. We have the following main result:

**Theorem 1.** Let $p$ be an odd prime, $n$ positive integer and $Q$ be a nonsingular quadratic form. Let $V = V_{p^3}(Q)$ be the set of integral solutions of the congruence (1) in $\mathbb{Z}_{p^3}$, and $B$ be a box as given in (2) centered at the origin with all $m_i \leq p^3$. If $\Delta = \pm 1$. Then

$$|B \cap V_{p^3}| \leq \left\{ \begin{array}{ll} \frac{|B|^3}{3\cdot n^{(2-n)/2}} & \text{if } \Delta = -1, \\ \frac{|B|^3}{3\cdot n^{(2-n)/2}} & \text{if } \Delta = +1, \\ \end{array} \right.$$  \quad (3)

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

$$u_n = \left\{ \begin{array}{ll} 2^n \left(1 + \frac{2}{3} n^{(2-n)/2}\right) & \Delta = -1, \\ 2^n \left(1 + \frac{2}{3} n^{(2-n)/2}\right) & \Delta = +1. \\ \end{array} \right.$$  \quad (4)


We shall devote the last section to give the proof of Theorem 1. If $V$ is the set of zeros of a nonsingular quadratic form $Q(x)$, then one can show that

$$|V \cap B| \geq \frac{|B|^3}{p} + O\left(p^{n/2}(\log p)^{3n}\right),$$  \quad (5)

for any box $B$ (see Cochrane [1984] and Hakami [2009]). It is apparent from (5) that $|V \cap B|$ is nonempty provided

$$|B| \gg p^{n/2+1}(\log p)^{3n}.$$  \quad (6)

In order to show that $\mathbb{B} \cap V$ is nonempty we can proceed as follows. Let $\alpha(x)$ be a complex valued function on $\mathbb{Z}_{p^3}$, such that $\alpha(x) \leq 0$ for all $x$ not in $\mathbb{B}$. If $\alpha(x)$ is nonempty, then it will follow that $\mathbb{B} \cap V$ is nonempty. Now $\alpha(x)$ has a finite Fourier expansion

$$\alpha(x) = \sum_{y} a(y) e_{p^3}(y \cdot x),$$

where

$$a(y) = p^{-3n} \sum_{x} \alpha(x) e_{p^3}(-y \cdot x),$$

Corresponding Author Email: aalhakami@jazanu.edu.sa
for all $y \in \mathbb{Z}_p^n$. Thus

$$\sum_{x \in V} a(x) = \sum_{x \in V} \sum_{y} a(y) e_{p^j}(y \cdot x) = \sum_{y} a(y) \sum_{x \in V} e_{p^j}(y \cdot x) = a(0) |V| + \sum_{y \neq 0} a(y) \sum_{x \in V} e_{p^j}(y \cdot x).$$

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

$$\sum_{x \in V} a(x) = p^{-3n} |V| \sum_{x} a(x) + \sum_{y} a(y) \phi(V, y), \quad (7)$$

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

$$\sum_{x \in V} a(x) = p^{-3} \sum_{x} a(x) + \sum_{y} a(y) \phi(V, y), \quad (8)$$

which is obtained from (7) by noticing that $|V| = \phi(V, 0) + p^{3(n-1)}$, whence

$$\sum_{x \in V} a(x) = a(0) [\phi(V, 0) + p^{3(n-1)}] + \sum_{y} a(y) \phi(V, y) = p^{-3a} a(0) + \sum_{y} a(y) \phi(V, y).$$

Equations (7) and (8) express the incomplete sum $\sum_{x \in V} a(x)$ as a fraction of the complete sum $\sum x a(x)$ plus an error term. In general $|V| = p^{3(n-1)}$ so that the fractions in the two equations are about the same. In fact, if $V$ is defined by a nonsingular quadratic form $Q(x)$ then $|V| = p^{3(n-1)} + O(p^n)$ (that is $|\phi(V, 0)| \ll p^n$).

To show that $\sum_{x \in V} a(x)$ is positive, it suffices to show that the error term is smaller in absolute value than the (positive) main term on the right-hand side of (7) or (8). One tries to make an optimal choice of $a(x)$ in order to minimize the error term. Special cases of (7) and (8) have appeared a number of times in the literature for different types of algebraic sets $V$; see [Chalk 1963, Tietäväinen 1967, and Myerson 1991]. The first case treated was to let $a(x)$ be the characteristic function $\chi_S(x)$ of a subset $S$ of $\mathbb{Z}_p^n$, whence (8) gives rise to formulas of the type

$$|V \cap S| = p^{-3} |S| + \text{Error}.$$

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

$$a * \beta(x) = \sum_{u} a(u) \beta(x - u) = \sum_{u+v=x} a(u) \beta(v),$$

for $x \in \mathbb{Z}_p^n$. If we take $a(x) = \chi_S * \chi_T(x)$ then it is clear from the definition that $a(x)$ is the number of ways of expressing $x$ as a sum $s + t$ with $s \in S$ and $t \in T$. Moreover, $(S + T) \cap V$ is nonempty if and only if $\sum_{x \in V} a(x) > 0$.

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

$$\sum_{x \in \mathbb{Z}_p^n} e_{p^j}(x \cdot y) = \begin{cases} p^{3n}, & y = 0, \\ 0, & y \neq 0, \end{cases}$$

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

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

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

$$a(x) = \sum_y a(y) e_{p^j}(x \cdot y), \quad \beta(x) = \sum_y b(y) e_{p^j}(x \cdot y).$$

Then

$$a \ast \beta(x) = \sum_y a(y) b(y) e_{p^j}(x \cdot y), \quad (9)$$

$$a(\beta(x)) = a(\beta(x)) \sum_y (a * b)(y) e_{p^j}(x \cdot y), \quad (10)$$

$$\sum_x \left[ (a * \beta)(x) \right] = \left[ \sum_x (a(x)) \right] \left[ \sum_x (\beta(x)) \right], \quad (11)$$

$$\sum_x \left[ (a * \beta)(x) \right] ^2 \leq \sum_x (|a(x)|^2) \left[ \sum_x (|\beta(x)|^2 \right], \quad (12)$$

$$\sum_x |a(y)|^2 = p^{-3n} \sum_x |a(x)|^2. \quad (13)$$

The last identity is Parseval’s equality.

**Fundamental Identity**

Let $Q(x) = Q(x_1, ..., x_n)$ be a quadratic form with integer coefficients and $p$ be an odd prime. Consider the congruence (1):

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

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

**Lemma 1.** [Hakami 2012, Theorem 1] Suppose $n$ is even, $Q$ is nonsingular (mod $p$) and $\Delta = \Delta_p(Q)$. For $y \in \mathbb{Z}_p^n$, put $y' = p^3 y$ in case $p \mid y$, (i.e., $p \mid y$ for all $i$). Then

$$\phi(V, y) = \rho^{3n/2 - 3} \sum_{x=0}^{2} \delta \rho^{m/2} \omega_{y'}(y'),$$

where $\delta$ is a constant depending on $\Delta$ and $\rho = \rho_p$.
with
\[
\delta_j = \begin{cases} 
1 & \text{if } 3 - j \text{ is even}, \\
\Delta & \text{if } 3 - j \text{ is odd},
\end{cases}
\]
and
\[
\omega_j(y') = \begin{cases} 
p^{\gamma - j} - p^{2j - 1}, & p^{\gamma - j} | Q'(y'), \\
p^{2j - 1}, & p^{\gamma} | Q'(y'), \\
0, & p^{\alpha} \nmid Q'(y'),
\end{cases}
\]
where \(Q'\) is the quadratic form associated with the inverse of the matrix for \(Q \pmod{p}\).

Back to (8) we saw the identity
\[
\sum_{x \in V_p^*} \alpha(x) = p^{-3} \sum_x \alpha(x) + \sum_{y \in 0} a(y) \phi(V,y).
\]
Inserting the value \(\phi(V,y)\) in Lemma 1 yields (see Hakami (2011d)).

**Lemma 2. (The fundamental identity)** For any complex valued \(\alpha(x)\) on \(\mathbb{Z}_p^*\), if \(\Delta = +1\), then
\[
\sum_{x \in V_p^*} \alpha(x) = p^{-3} \sum_x \alpha(x) + p^{3n/2} \sum_{y \in 1} a(y)
+ p^{2n-1} \sum_{y \in \overline{Q'}} a(py) + p^{(3n/2)-2} \sum_{y \in \overline{Q'}} a(p^2y)
- p^{3(n/2)-2} \sum_{y \in \overline{Q'}} a(y) - p^{2n-2} \sum_{y \in \overline{Q'}} a(py)
- p^{5(n/2)-3} \sum_{y \in \overline{Q'}} a(p^2y).
\]

If \(\Delta = -1\), then
\[
\sum_{x \in V_p^*} \alpha(x) = p^{-3} \sum_x \alpha(x) - p^{3n/2} \sum_{y \in \overline{Q'}} a(y)
+ p^{2n-1} \sum_{y \in \overline{Q'}} a(py) - p^{(3n/2)-2} \sum_{y \in \overline{Q'}} a(p^2y)
+ p^{3(n/2)-2} \sum_{y \in \overline{Q'}} a(y) - p^{2n-2} \sum_{y \in \overline{Q'}} a(py)
+ p^{5(n/2)-3} \sum_{y \in \overline{Q'}} a(p^2y).
\]

**Auxiliary lemmas**

For later reference, we construct the following two lemmas on estimating the sum \(\sum_{y \in 0} a(py)\) and \(\sum_{y \in 1} p^3 a(p^2y)\). Let \(B\) be a box of points in \(\mathbb{Z}^n\) as in (2) centered about the origin with all \(m_i \leq p\), and view this box as a subset of \(\mathbb{Z}_p^*\). Let \(\chi_B\) be its characteristic function with Fourier expansion \(\chi_B(x) = \sum_y a(y) \epsilon_{p^e}(x \cdot y)\). Let \(\alpha(x) = \chi_B \ast \chi_B = \sum_y a(y) \epsilon_{p^e}(x \cdot y)\). Then for any \(y \in \mathbb{Z}_p^n\),
\[
a(y) = p^{-3n} \prod_{i=1}^n \left( \frac{\sin^2 \left( \pi m_i y_i / p^3 \right)}{\sin^2 \left( \pi y_i / p^3 \right)} \right).
\]
where the term in the product is taken to be \(1\) if \(y_i = 0\).

**Lemma 3.** Let \(B\) be any box of type (2) viewed as a subset of \(\mathbb{Z}_p^n\) and \(\alpha(x) = \chi_B \ast \chi_B(x)\). Then we have
\[
\sum_{y \in 0} p^3 a(py) \leq \frac{|B|}{p^2} \prod_{m_i \geq p^3} 2m_i / p^2.
\]

**Proof.** First,
\[
\sum_{y \in 0} p^3 a(py) = \sum_{y \in 1} \sum_{y \in \overline{Q'}} \frac{1}{p^3} \alpha(x) \epsilon_{p^e}(-x \cdot py)
= \sum_{x \in \overline{Q'}} \sum_{y \in \overline{Q'}} \frac{1}{p^3} \alpha(x) \epsilon_{p^e}(-x \cdot y)
= \frac{1}{p^3} \sum_{x \equiv 0 \pmod{p^3}} \alpha(x)
= \frac{1}{p^3} \sum_{u \equiv v \pmod{p^3}} 1.
\]
Now we need to count the number of solutions of the congruence
\[u + v \equiv 0 \pmod{p^3},\]
with \(u, v \in B\). In fact for each choice of \(v\), there are at most \(\prod_{i=1}^n (|m_i/p^3| + 1)\) choices for \(u\). So the total number of solutions is less than or equal to \(\prod_{i=1}^n m_i (|m_i/p^3| + 1)\). It follows from (16),
\[
\sum_{y \in 0} p^3 a(py) \leq \frac{1}{p^3} \prod_{i=1}^n m_i \left( \frac{|m_i|}{p^3} + 1 \right). \tag{17}
\]
We split the product in (17) to get
\[
\prod_{i=1}^n m_i \left( \frac{|m_i|}{p^3} + 1 \right) \leq \prod_{m_i < p^3} m_i \prod_{m_i \geq p^3} m_i \left( \frac{|m_i|}{p^3} + 1 \right).
\]
Then by help of this inequality we obtain

\[
\sum_{y=1}^{p} \alpha(p^2y) \leq \frac{1}{p^2} \prod_{m_i < p^2} m_i \prod_{m_i \geq p^2} \left( \frac{m_i}{p^2} + 1 \right) \\
\leq \frac{|\mathcal{B}|}{p^{n}} \prod_{m_i \geq p^2} \frac{2m_i}{p^2},
\]

proving the lemma. □

**Lemma 4.** Let \( \mathcal{B} \) be any box of type \( 2 \) and \( \alpha(x) = \chi_\mathcal{B} \ast \chi_\mathcal{B}(x) \). Then we have

\[
\sum_{y=1}^{p} \alpha(p^2y) \leq \frac{|\mathcal{B}|}{p^{n}} \prod_{m_i \geq p^2} \frac{2m_i}{p^2}.
\]

**Proof.** The idea of the proof is exactly similar to the ideas used to prove Lemma 3. □

**Proof of Theorem 1**

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

\[
\mathcal{B} = \{ x \in \mathbb{Z}^n \mid a_i \leq x_i < a_i + m_i, \ 1 \leq i \leq n \}
\]

where \( a_i, m_i \in \mathbb{Z}, \ 1 \leq m_i \leq p^3, \ 1 \leq i \leq n \). Then \( |\mathcal{B}| = \prod_{i=1}^{n} m_i \), the cardinality of \( \mathcal{B} \). View the box \( \mathcal{B} \) as a subset of \( \mathbb{Z}^n_p \), and let \( \chi_\mathcal{B} \) be its characteristic function with Fourier expansion \( \chi_\mathcal{B}(x) = \sum_{y} \alpha(y)e_p(x \cdot y) \).

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

Consider the congruence (1) and consider (15), the fundamental identity (mod \( p^n \)) when \( \Delta = -1 \):

\[
\sum_{x \in \mathcal{V}_p} \alpha(x) = p^{-3} \sum_{x} \alpha(x) - p^{3n/2} \sum_{y=1}^{p^3} \alpha(y)
+ p^{2n-1} \sum_{y=1}^{p^3} \alpha(py) - p^{3n/2-2} \sum_{y=1}^{p^{3n/2}} \alpha(p^2y)
+ p^{3n/2-1} \sum_{y=1}^{p^{3n/2}} \alpha(y) - p^{2n-2} \sum_{y=1}^{p^{3n/2}} \alpha(py)
+ p^{3n/2-3} \sum_{y=1}^{p^{3n/2}} \alpha(p^2y).
\]

Put \( \alpha = \chi_\mathcal{B} \ast \chi_\mathcal{B} = \sum_{y} \alpha(y)e_p(x \cdot y) \). Then the Fourier coefficients of \( \alpha(x) \) are given by \( \alpha(y) = p^{3n} \alpha(y) \) and by Parseval’s identity satisfy

\[
\sum_{y} |\alpha(y)|^2 = \sum_{y} |\alpha(y)|^2 = |\mathcal{B}|. \quad (18)
\]

Consequently from (18),

\[
p^{3n/2-1} \sum_{y=1}^{p^3} \alpha(y) \leq p^{3n/2-1} \sum_{y} |\alpha(y)| \leq p^{3n/2-1} |\mathcal{B}|. \quad (19)
\]

Besides this we have that the main term in (15) is

\[
p^{-3} \sum_{x} \alpha(x) = p^{-2} \sum_{x} \chi_\mathcal{B} \ast \chi_\mathcal{B}(x) = \frac{|\mathcal{B}|^2}{p^3}. \quad (20)
\]

Also we have by Lemma 3,

\[
p^{2n-1} \sum_{y=1}^{p^3} \alpha(py) \leq p^{2n-1} \sum_{y=1}^{p^{3n/2}} \alpha(p^2y) = p^{2n-1} \sum_{y=1}^{p^{3n/2}} \alpha(y)
= p^{n-1} |\mathcal{B}| \prod_{m_i \geq p^2} \frac{2m_i}{p^2}, \quad (21)
\]

and by Lemma 4,

\[
p^{(3n/2)-3} \sum_{y=1}^{p^3} \alpha(p^2y) \leq p^{(3n/2)-3} |\mathcal{B}| \prod_{m_i \geq p^2} \frac{2m_i}{p^2}
= p^{(n/2)-3} |\mathcal{B}| \prod_{m_i \geq p^2} \frac{2m_i}{p^2}. \quad (22)
\]

Now turn back to (15), we have

\[
\sum_{x \in \mathcal{V}_p} \alpha(x) \leq p^{-3} \sum_{x} \alpha(x) + p^{3n/2-1} \sum_{y=1}^{p^3} \alpha(y)
+ p^{2n-1} \sum_{y=1}^{p^3} \alpha(py) + p^{3n/2-3} \sum_{y=1}^{p^{3n/2}} \alpha(p^2y). \quad (23)
\]

Then by inequalities in (20), (19), (21), and (22) we obtain

\[
\sum_{x \in \mathcal{V}_p} \alpha(x) \leq \frac{|\mathcal{B}|^2}{p^3} + p^{3n/2-1} |\mathcal{B}| + p^{n-1} |\mathcal{B}| \prod_{m_i \geq p^2} \frac{2m_i}{p^2}
+ p^{(n/2)-3} |\mathcal{B}| \prod_{m_i \geq p^2} \frac{2m_i}{p^2}. \quad (24)
\]

But, it easily to see that

\[
\sum_{x \in \mathcal{V}_p} \alpha(x) \geq \frac{1}{2^n} |\mathcal{B}| |\mathcal{V}_p \cap \mathcal{B}|. \quad (25)
\]

Thus we have (by (24) and (25))

\[
|\mathcal{V}_p \cap \mathcal{B}| = 2^n \left( \frac{|\mathcal{B}|}{p^3} + p^{(3n/2)-1} + p^{n-1} \prod_{m_i \geq p^2} \frac{2m_i}{p^2}
+ p^{(n/2)-3} \prod_{m_i \geq p^2} \frac{2m_i}{p^2} \right). \quad (26)
\]
The task now is designation which of the terms \( \frac{[g]}{p^3} \),
\( p^{n-1} \prod_{m_i \geq p^2} \frac{2m_i}{m_i} \) and \( p^{(n/2)-3} \prod_{m_i \geq p} \frac{2m_i}{m_i} \) in (26) is the dominant term. We consider two cases:

**Case (i):** We define \( l \) by
\[
m_1 \leq m_2 \leq \cdots \leq m_i < p^2 \leq m_{i+1} \leq \cdots \leq m_n.
\]
Then

I. Assume \( l \leq \frac{n}{2} - 1 \). Then compare
\[
\frac{p^{n-1} \prod_{m_i \geq p^2} \frac{2m_i}{m_i}}{p^{3(n/2)-1}} = \frac{2^{n-1} p^{n/2}}{p^{3(n/2)-1}} \leq \frac{2 \cdot [g]}{p^3}.
\]

II. Assume \( l \geq \frac{n}{2} \). Then compare
\[
\frac{p^{n-1} \prod_{m_i \geq p^2} \frac{2m_i}{m_i}}{p^{3(n/2)-1}} = \frac{1}{p^{3/2}} \prod_{m_i \geq p^2} \frac{2m_i}{m_i} \leq \frac{1}{p^{3/2}} \prod_{m_i \geq p^2} 2p \leq \frac{2^{n/2}}{2p^{3/2}} = 2^{n/2},
\]
which implies that
\[
p^{n-1} \prod_{m_i \geq p^2} \frac{2m_i}{m_i} \leq 2^{n/2} p^{(3n/2)-1}.
\]
We get by (I) and (II) that
\[
p^{n-1} \prod_{m_i \geq p^2} \frac{2m_i}{m_i} \leq \max \left( 2^n \frac{[g]}{p^3}, 2^{n/2} p^{(3n/2)-1} \right) \leq 2^n \frac{[g]}{p^3} + 2^{n/2} p^{(3n/2)-1}.
\]

**Case (ii):** We define \( l' \) by
\[
m_1 \leq m_2 \leq \cdots \leq m_i < p \leq m_{i+1} \leq \cdots \leq m_n.
\]
Then

III. Assume \( l' \leq \frac{n}{2} - 1 \). Then compare
\[
\frac{p^{(n/2)-3} \prod_{m_i \geq p} \frac{2m_i}{m_i}}{p^{3(n/2)-1}} = \frac{2^{n-l} p^{n/2}}{p^{3(n/2)-1}} = \frac{2^n}{p^{n/2}} \left( \frac{p}{2} \right)^{l'} \leq \frac{2^n}{p^{n/2}} \left( \frac{p}{2} \right)^{(n/2)-1} \leq \frac{2^{n/2} + 2^{n/2}}{p^2} p^{(3n/2)-1},
\]
leads to
\[
p^{(n/2)-3} \prod_{m_i \geq p} \frac{2m_i}{m_i} \leq \frac{2^{n+1} \cdot [g]}{p^{3(n/2)-1}}.
\]

IV. Assume \( l' \geq \frac{n}{2} \). Then compare
\[
\frac{p^{(n/2)-3} \prod_{m_i \geq p} \frac{2m_i}{m_i}}{p^{3(n/2)-1}} = \frac{1}{p^{3/2}} \prod_{m_i \geq p^2} \frac{2m_i}{m_i} \leq \frac{1}{p^{3/2}} \prod_{m_i \geq p^2} 2p \leq \frac{2^{n/2}}{2p^{3/2}} = 2^{n/2},
\]
implies that
\[
p^{(n/2)-3} \prod_{m_i \geq p} \frac{2m_i}{m_i} \leq 2^{n/2} p^{(3n/2)-1}.
\]
Thus by (III) and (IV),
\[
p^{(n/2)-3} \prod_{m_i \geq p} m_i \leq 2^{n+1} \frac{[g]}{p^3} + \frac{2^{n/2}}{p^2} p^{(3n/2)-1}.
\]
Together, case (i) and case (ii) gives us
\[
p^{n-1} \prod_{m_i \geq p^2} \frac{2m_i}{m_i} + p^{(n/2)-3} \prod_{m_i \geq p} \frac{2m_i}{m_i} \leq \left( 2^n + \frac{2^{n+1}}{p} \right) \frac{[g]}{p^3} + \left( 2^{n/2} + \frac{2^{n/2}}{p^2} \right) p^{(3n/2)-1}.
\]
We conclude by making use of (26) to get

$$\left| V_{p^{k}} \cap B \right| \leq 2^{n}\left(\frac{|B|}{p} + p^{(3n/2)-1} + p^{n-1} \prod_{m_i \geq p^2} \frac{2m_i}{p^2} \right.\left. + \frac{p^{n(2)-3}}{p} \prod_{m_i \geq p} 2m_i \right) \leq 2^{n}\left(\frac{|B|}{p} + p^{(3n/2)-1} + \left\{p^{(2n/2)\frac{2n}{p}} + \left(2n^2 + \frac{2n}{p}\right)p^{(3n/2)-1}\right\} \right) \leq 2^{n}\left(1 + 2^{n} + \frac{2n(2n+1)}{p}\right) + 2^{n}\left(1 + 2n^2 + \frac{2n(2n+1)}{p}\right)p^{(3n/2)-1} \leq v'_n\left(\frac{|B|}{p} + p^{(3n/2)-1}\right),$$

where $v'_n = 2^n \left(1 + 2^n + \frac{2n(2n+1)}{p}\right)$.

**The case $\Delta = +1$:**

We now examine the case $\Delta = +1$. Appealing to (14), we obtain

$$\sum_{x \in V_{p^k}} \alpha(x) \leq p^{-3} \sum_{x} \alpha(x) + p^{3n/2} \sum_{p^j \mid q^j(y')} a(y')$$

$$+ p^{2n-1} \sum_{p^j \mid q^j(y')} a(p^jy') + p^{(5n/2)-2} \sum_{p^j \mid q^j(y')} a(p^jy')$$

$$\leq \frac{|B|^2}{p^3} + p^{3n/2} |B| + p^{2n-1} \frac{|B|}{p} \prod_{m_i \geq p^2} \frac{2m_i}{p^2}$$

$$+ p^{(5n/2)-2} \frac{|B|}{p^2} \prod_{m_i \geq p} \frac{2m_i}{p}.$$  

But, once again by (26), we obtain

$$\left| V_{p^k} \cap B \right| = 2^n\left(\frac{|B|}{p} + p^{(3n/2)} + p^{n-1} \prod_{m_i \geq p^2} \frac{2m_i}{p^2} \right.\left. + p^{(n/2)-2} \prod_{m_i \geq p} \frac{2m_i}{p} \right).$$

We do a similar investigation (as before) to determine which of the quantities $\frac{|B|}{p}$, $p^{3n/2}$, $p^{(n/2)-1} \prod_{m_i \geq p} \frac{2m_i}{p}$ and $p^{(n/2)-2} \prod_{m_i \geq p} \frac{2m_i}{p}$ of (27) is the dominant term. Indeed in case (i) $l \leq \frac{n}{2} - 1$, we have (as we saw earlier) $p^{n-1} \prod_{m_i \geq p^2} \frac{2m_i}{p^2} \leq 2^{n} \frac{|B|}{p^3}$, and when $l \leq \frac{n}{2}$,

$$\frac{p^{n-1} \prod_{m_i \geq p^2} \frac{2m_i}{p^2}}{p^{3n/2}} \leq \frac{1}{p^{n(2)+1}} \prod_{m_i \geq p} 2p \leq \frac{1}{p^{n(2)+1}} (2p)^{n/2} = \frac{2^{n/2}}{p},$$

which means $p^{n-1} \prod_{m_i \geq p} \frac{2m_i}{p^2} \leq \frac{2^{n/2}}{p} p^{3n/2}$. We therefore obtain

$$p^{n-1} \prod_{m_i \geq p} \frac{2m_i}{p^2} \leq \max \left\{\frac{|B|}{p^3}, \frac{2^{n/2}}{p^{2}} p^{3n/2}\right\} \leq \frac{2^n}{p^3} + \frac{2^{n/2}}{p^{2}} p^{3n/2}.$$  

In case (ii) when $l' \leq \frac{n}{2} - 1$, we have

$$\frac{p^{l}\prod m_{i} \geq p \frac{2m_{i}}{p}}{p^{3n/2}} = \frac{2^{n-l} p^{l} \prod m_{i} \geq p m_{i}}{p^{3n/2}} = \frac{2^{n-l} \prod m_{i} \geq p m_{i}}{p^{3n/2}}$$

which means $p^{n-2} \prod_{m_i \geq p} \frac{2m_i}{p} \leq \frac{2^{n/2}}{p} p^{3n/2}$. When $l' \leq \frac{n}{2}$,

$$\frac{\prod m_{i} \geq p \frac{2m_{i}}{p}}{p^{3n/2}} = \frac{1}{p^{n+1}} \prod m_{i} \geq p \frac{2m_{i}}{p} \leq \frac{1}{p^{n+1}} \prod m_{i} \geq p 2p^2 \leq \frac{1}{p^{n+1}} (2p^2)^{n/2} = \frac{2^n}{p^3},$$

which means $p^{n-2} \prod_{m_i \geq p} \frac{2m_i}{p} \leq \frac{2^{n/2}}{p} p^{3n/2}$. Thus we get

$$p^{n-2} \prod m_{i} \geq p \frac{2m_{i}}{p} \leq 2^{n+1} \frac{|B|}{p^3} + \frac{2^{n/2}}{p^3} p^{3n/2}.$$
Putting case (i) and case (ii) together, we obtain

\[ |V_p \cap B| \leq 2^n \left( \frac{2^n}{p} + p^{3n/2} + P^n-1 \prod_{m \geq p^2} \frac{2m}{p} \right. \\
\left. + \frac{2^{m-p^2}}{p} \prod_{m \geq p^2} \frac{2m}{p} \right) \]

\[ \leq 2^n \left( \frac{2^n}{p} + p^{3n/2} + \left( 2^n + 2^{(n/2)+1} \right) \frac{2^n}{p} \right) \\
\leq 2^n \left( 1 + 2^n + 2^{(n/2)+1} \right) \frac{2^n}{p} + 2^n \left( 1 + 2^{(n/2)} + 2^{(n/2)} \right) p^{3n/2} \\
= \nu_n \left( \frac{2^n}{p} + p^{3n/2} \right), \]

where \( \nu_n = 2^n \left( 1 + 2^n + 2^{(n/2)+1} \right) \)

Lastly let \( \nu_n = \nu' \) if \( \Delta = -1 \) and \( \nu_n = \nu'' \) if \( \Delta = +1 \) to conclude the proof of Theorem 1.

Acknowledgements

The author is most grateful to the referee and the editors especially Professor Tin-Yan Tam who handle this paper. He would also like to thank his colleague Professor Idir MECHAI for his assistance in formatting and typesetting this paper.

References


