§1. Introduction.

Let \( Q(x) = Q(x_1, x_2, \ldots, x_n) \) be a quadratic form with integer coefficients and \( m = pq \), a product of distinct primes. Heath-Brown [5, Theorem 1] proved that for \( n \geq 4 \) and any \( \epsilon > 0 \) the congruence

\[
Q(x) \equiv 0 \mod m
\]

has a nonzero solution with \( \max |x_i| \ll m^{\frac{1}{2} + \epsilon} \), which was an improvement on the result of Cochrane [1]. We shall prove here a best possible result, namely that for \( n \geq 4 \) the congruence (1) has a nonzero solution with \( \max |x_i| \ll m^{\frac{1}{2}} \), generalizing the result of Cochrane [2] for prime moduli.

Indeed, following the line of argument in Heath-Brown's work, we shall prove the analogous result for an arbitrary box centered at the origin. Let

\[
B = \{ x \in \mathbb{Z}^n : |x_i| \leq B_i, 1 \leq i \leq n \}
\]

where the \( B_i \) are nonnegative integers. Set \( b_i = 2B_i + 1 \), \( 1 \leq i \leq n \), and \( |B| = \Pi_{i=1}^{n} b_i \); the cardinality of \( B \).

**Theorem.** Let \( Q \) be any quadratic form in \( n \geq 4 \) variables over \( \mathbb{Z} \) and \( m = pq \) a product of distinct primes. Then any box \( B \) as in (2) with

\[
|B| > 2^{50n} m^{n/2}
\]

contains a nonzero solution of (1).

Further difficulties are encountered for a general modulus using the method given here. In particular, one needs to be able to obtain an upper bound as in (13) for any square free \( m \) comprised of primes \( p \) with \( \Delta_p(Q) = -1 \). Schinzel, Schlickewei and Schmidt [6], Heath-Brown [5] and Cochrane [3], have obtained results for a general modulus \( m \), but they all (likely) fall short of being best possible. (No attempt was made to get the best possible constant in (3).)

\(^1\) Research was supported by the United States National Security Agency.
§2. Prime Moduli.

We begin by considering the case of a prime modulus. If $n$ is even and $p$ is an odd prime then we set

$$
\Delta_p(Q) = \left( \frac{(-1)^{\frac{n}{2}} \det Q}{p} \right)
$$

if $p \nmid \det Q$ and $\Delta_p(Q) = 0$ if $p | \det Q$. Here, $\left( \frac{\cdot}{p} \right)$ denotes the Legendre symbol. The following lemma is just a special case of Theorem 2 of [2].

**LEMMA 1.** Suppose that $n \geq 4$ is even, $p > 2^{4n+6}10^{2n-2}$, and that $\Delta_p(Q) = -1$. Let $B$ be a box as in (2) with $2^{5n+7}10^n \leq b_i \leq p$ for $1 \leq i \leq n$ and

$$
|B| > 2^{3n^2+4n+2+10n}p^\frac{n}{2}.
$$

Then $B$ contains a nonzero point $x$ with $p|Q(x)$. (This lemma holds for boxes not centered at the origin as well.)

**LEMMA 2.** Suppose that $n \geq 4$, and that $B$ is a box as in (2) with

$$
|B| > 2^{2n}p^\frac{n}{2}.
$$

Then $B$ contains a nonzero point $x$ with $p|Q(x)$.

**PROOF:** Suppose first that $n = 4$ and that $B$ satisfies (5). If $\Delta_p(Q) = 0$ or 1 then the congruence

$$
Q(x) \equiv 0 \mod p
$$

has a lattice of solutions of determinant $p^2$ and hence, by Minkowski’s theorem, it has a nonzero solution in $B$.

Suppose now that $\Delta_p(Q) = -1$. If $B_i \geq p$ for some $i$ then $B$ contains the trivial (but nonzero) solution $x$ with $x_i = p$ and $x_j = 0$ for $j \neq i$. Thus we may assume that $B_i < p$ for all $i$. In particular, this implies that $p > 2^{22}10^6$, for if $p \leq 2^{22}10^6$ then by (5) some $b_i > 2^{22}p^\frac{3}{2} > 2p$.

For any $B_i > \frac{p}{2}$ we replace $B_i$ with $\frac{p-1}{2}$ and form a new box $B' = \{ x \in \mathbb{Z}^4 : |x_i| \leq B'_i, 1 \leq i \leq 4 \}$, where $B'_i = \min \{ B_i, \frac{p-1}{2} \}$, $b'_i = 2B'_i + 1$. We note that $b'_i \leq p$ for $1 \leq i \leq 4$ and that

$$
|B'| > \Pi_{i=1}^4 \frac{b'_i}{2} > 2^{84}p^2.
$$

If $b'_i \geq 2^{27}10^4$ for $1 \leq i \leq 4$, then by Lemma 1 $B'$ contains a nonzero solution of (6). If $b'_i < 2^{27}10^4$ for some $i$, say $i = 1$, then we set $x_1 = 0$ and consider the form $Q_1(x_2, x_3, x_4) = Q(0, x_2, x_3, x_4)$.

The congruence $Q_1 \equiv 0 \mod p$ has a lattice of solutions in $\mathbb{Z}^3$ of determinant $p^2$. Now $b'_{b'_3b'_4} = |B'|/b'_1 > 2^{41}p^2$, and so by Minkowski’s theorem there is a nonzero point $(x_2, x_3, x_4)$ in the lattice with $|x_i| \leq B'_i$, $2 \leq i \leq 4$. Then $(0, x_2, x_3, x_4)$ is a nonzero solution of (6) in $B$. 

2
Suppose now that \( n \geq 4 \) and that, without loss of generality, \( b_1 \geq b_2 \cdots \geq b_n \). Set \( Q_2(x_1, x_2, x_3, x_4) = Q(x_1, x_2, x_3, x_4, 0, 0, \ldots, 0) \). Then by (5) we have

\[
\prod_{i=1}^{4} b_i \geq (\prod_{i=1}^{n} b_i)^{4/n} > 2^{88} p^2,
\]

and so there is a nonzero point \( (x_1, x_2, x_3, x_4) \) with \( p|Q_2(x_1, x_2, x_3, x_4) \), and \( |x_i| \leq B_i \) for \( 1 \leq i \leq 4 \). Then \( (x_1, x_2, x_3, x_4, 0, 0, \ldots, 0) \) is the desired solution of (6).


As in the proof of Lemma 2 we may assume that \( n = 4 \) and that \( 0 \leq B_i < \frac{m}{2} \) for \( 1 \leq i \leq 4 \). Also, we may assume that \( p \) and \( q \) are odd. Let \( B \) be a box as in (2) satisfying \( |B| > 2^{200} m^2 \).

Case i: Suppose that \( \Delta_p = 0 \) or 1 or that \( \Delta_q = 0 \) or 1, say without loss of generality that the former holds. In this case we simply reproduce the elegant argument of Heath-Brown [5, §2]. Let \( \mathcal{L} \) be a lattice of solutions of (6) of determinant \( p^2 \). Let \( \overline{B} \) be the solid box of points in \( \mathbb{R}^4 \) with \( |x_i| \leq B_i + \frac{1}{2} \), \( 1 \leq i \leq 4 \). Then by the theorem on successive minima, there are positive values \( \lambda_1, \lambda_2, \lambda_3, \lambda_4 \) such that \( \lambda_i \overline{B} \) contains \( i \) linearly independent points of \( \mathcal{L} \), \( 1 \leq i \leq 4 \), and

\[
\prod_{i=1}^{4} \lambda_i \leq 2^4 p^2 / |B|.
\]

Let \( v_1, v_2, v_3, v_4 \) be linearly independent points of \( \mathcal{L} \) with \( v_i = (v_{i1}, v_{i2}, v_{i3}, v_{i4}) \in \lambda_i \overline{B} \), so that \( |v_{ij}| \leq \lambda_i (B_j + \frac{1}{2}) \) for \( 1 \leq i, j \leq 4 \).

Set \( F(y_1, y_2, y_3, y_4) = Q \left( \sum_{i=1}^{4} y_i v_i \right) \). Now

\[
\prod_{i=1}^{4} \frac{1}{4\lambda_i} \geq 2^{-12} |B| / p^2 > 2^{138} q^2,
\]

and so by Lemma 2 there is a nonzero point \( (y_1, y_2, y_3, y_4) \) with \( q|F(y_1, y_2, y_3, y_4) \) and \( |y_i| \leq \frac{1}{4\lambda_i} \), \( 1 \leq i \leq 4 \). Then for \( 1 \leq j \leq 4 \), \( |\sum_{i=1}^{4} y_i v_{ij}| \leq B_j \), and so \( \sum_{i=1}^{4} y_i v_i \) is a nonzero point in \( B \) satisfying (1).

Case ii: Suppose that \( \Delta_p = \Delta_q = -1 \). If \( B_i < 2^{64} \) for some \( i \), say \( i = 1 \), then we set \( x_i = 0 \) and \( Q_1(x_2, x_3, x_4) = Q(0, x_2, x_3, x_4) \). The congruence \( Q_1 \equiv 0 \mod m \) has a lattice of solutions in \( \mathbb{Z}^3 \) of determinant \( m^2 \). Since \( b_2 b_3 b_4 = |B| / b_1 \geq 2^{-65} |B| > 2^{138} m^2 \), it follows that there is a nonzero point \( (x_2, x_3, x_4) \) in this lattice with \( |x_i| \leq B_i \), \( 2 \leq i \leq 4 \). Thus we may assume that \( B_i \geq 2^{64} \) for all \( i \).

Suppose next that \( p < 2^{52} \) or \( q < 2^{52} \), say the former. Let

\[
B_1 = \left\{ x \in \mathbb{Z}^4 : x_i \leq \left\lfloor \frac{B_i}{p} \right\rfloor, \ 1 \leq i \leq 4 \right\}.
\]

Then (assuming \( B_i \geq 2^{64} \) for all \( i \))

\[
|B_1| \geq \prod_{i=1}^{4} \left( \frac{2B_i}{p} - 1 \right) > \prod_{i=1}^{4} \frac{B_i}{p} > \frac{|B|}{2^{8} p^4} \geq 2^{88} q^2.
\]
Thus, by Lemma 2, there is a nonzero point \( \mathbf{x} \in \mathcal{B}_1 \) with \( q|Q(\mathbf{x}) \). Then \( p \mathbf{x} \) is a nonzero solution of (1) in \( \mathcal{B} \).

Thus, we may assume from hereon that

\[
2^{64} \leq B_i < \frac{m}{2}, \quad 1 \leq i \leq 4,
\]

(7)

and that \( p, q > 2^{52} \). We will show that under these conditions, if

\[
|\mathcal{B}| \geq 2^{103}m^2
\]

(8)

then \( 2\mathcal{B} \) contains a nonzero solution of (1). The theorem follows on applying this result to the box \( \{ \mathbf{x} \in \mathbb{Z}^4 : |x_i| \leq [B_i/2] \} \).

In what follows it will be convenient to split the \( b_i \) into two sets, those with \( b_i \leq q \) and those with \( b_i > q \). Let \( s \) denote the cardinality of the first set and set

\[
\beta = \Pi_{b_i \leq q} b_i.
\]

(9)

Then by (8) we have \( \beta m^{4-s} \geq 2^{103}m^2 \), and so \( \beta \geq 2^{103}m^{s-2} \). If \( s \geq 2 \) it follows that

\[
\beta \geq 2^{103}q^{s-2}.
\]

(10)

If \( s = 0 \) then \( \beta = 1 > 2^{103}/q^2 \) (since \( q > 2^{52} \)), while if \( s = 1 \) then \( \beta = b_i > 2^{65} > 2^{103}/q \). Thus (10) holds for all \( s \).

§4. Exponential Sums. \( n = 4, \Delta_p(Q) = \Delta_q(Q) = -1 \).

Let \( \mathbb{Z}_m \) denote the residue class ring mod \( m \). We shall identify \( \mathbb{Z}_m \) with the set of integer representatives from \( -\left[ \frac{m}{2} \right] \) to \( \left[ \frac{m}{2} \right] \) and make similar identifications for \( \mathbb{Z}_p \) and \( \mathbb{Z}_q \). Thus if \( y \in \mathbb{Z}_m \) we can write \( |\sin(\pi y/m)| \geq |2y/m| \). Let \( e_m(\alpha) = e^{2\pi i \alpha/m} \) and \( x \cdot y = \sum_{i=1}^{4} x_i y_i \). We shall abbreviate complete sums \( \sum_{x \in \mathbb{Z}_m^4} \) by \( \sum_{x \in \mathbb{Z}_m} \). Let \( Q^* \) be the quadratic form associated with the inverse of the matrix representing \( Q \) mod \( m \). Let \( V_m, V_p \) and \( V_q \) denote the sets of zeros of \( Q \) in \( \mathbb{Z}_m^4, \mathbb{Z}_p^4 \) and \( \mathbb{Z}_q^4 \) respectively.

Let \( \mathcal{B} \) be a box of points as in (2) satisfying (7) and (8). Let \( \chi_{\mathcal{B}} \) denote the characteristic function of \( \mathcal{B} \) (viewed as a subset of \( \mathbb{Z}_m^4 \)) and \( \alpha = \chi_{\mathcal{B}} * \chi_{\mathcal{B}} \) the convolution of \( \chi_{\mathcal{B}} \) with itself,

\[
\alpha(\mathbf{x}) = \sum_{w \in \mathcal{B}} \sum_{\mathbf{x} \in \mathcal{B}} 1
\]

with Fourier expansion \( \alpha(\mathbf{x}) = \sum_{y(\mathbf{m})} a(y) e_m(\mathbf{x} \cdot \mathbf{y}) \). Then

\[
a(y) = m^{-4} \Pi_{i=1}^{4} \frac{\sin^2 \pi b_i y_i/m}{\sin^2 \pi y_i/m},
\]

where a term in the product is taken to be \( b_i^2 \) if \( y_i = 0 \). In particular,

\[
a(y) \leq m^{-4} \Pi_{i=1}^{4} \min \left( \frac{b_i^2}{m^2}, \frac{1}{2^2 y_i^2} \right).
\]

(11)
By Lemma 3 of [1] we have
\begin{equation}
\sum_{x \in V_m} a(x) \geq m^{-4}|V_m| \sum_{x \in (n)} a(x) - q^2|V_p| \sum_{Q^*(u) \equiv 0 \mod q} a(pu) \\
- p^2|V_q| \sum_{Q^*(v) \equiv 0 \mod p} a(qv) - p^2q \sum_{Q^*(y) \equiv 0 \mod p} a(y) \\
- pq^2 \sum_{Q^*(y) \equiv 0 \mod q} a(y),
\end{equation}

where \( u, v \) and \( y \) run through complete sets of residues \( \mod q, \mod p \) and \( \mod m \) respectively. Now,
\[
|V_m| = |V_p||V_q| = (p^3 - p^2 + p)(q^3 - q^2 + q) > m^3 \left( 1 - \frac{1}{p} \right) \left( 1 - \frac{1}{q} \right) > \frac{1}{2} m^3,
\]
and so the first term on the right-hand-side of (12) is greater than \( \frac{1}{2} |B|^2 / m \). Our goal is to show that the sum of the remaining four terms on the right-hand-side of (12) is less than \( \frac{2}{5} |B|^2 / m \), whence we have that
\[
\sum_{x \in V_m} a(x) \geq \frac{1}{10} \frac{|B|^2}{m} > |B| = \alpha(0),
\]
and conclude that \( 2B \) contains a nonzero solution of (1). By symmetry it is enough to consider just the second and fourth terms on the right-hand-side of (12) which we do in sections 5 and 6 respectively.

We shall make use of the following upper bounds which are taken from inequalities (9) and (10) of [2], (with \( t = 14 \)). Let \( B \) be a box as in (2) with all \( B_i < \frac{q}{2} \), viewed as a subset of \( \mathbb{Z}^4_q \). Then
\begin{equation}
|B \cap V_q| \leq 2^4 \left( \frac{|B|}{q} + q \right).
\end{equation}

If in addition \( B_i \leq 2^{-21} q \) for \( 1 \leq i \leq 4 \), then
\begin{equation}
|B \cap V_q| \leq 2^{85} \frac{|B|}{q} + 2^{-14} q.
\end{equation}

§5. The sum \( \sum^* a(pu) \).

In this section \( u \) runs through the set of representatives of \( \mathbb{Z}^4_q \) with \(- \frac{q}{2} < u_i < \frac{q}{2}\), \( 1 \leq i \leq 4 \). We shall abbreviate sums of the type \( \sum_{Q^*(u) \equiv 0 \mod q} \) by \( \sum^*_u \). For \( j = 1, 2, 3, 4 \) let \( \pi \) run through the set of injections of \( \{1, 2, \ldots, j\} \) into \( \{1, 2, 3, 4\} \) with \( \pi(h) < \pi(i) \) for \( h < i \). Thus
for any choice of \( j \) values from \( \{1, 2, 3, 4\} \) there is exactly one such mapping \( \pi \) taking on these values. Then, by (11), we have

\[
\sum_{Q^*(u) \equiv 0 \mod q} a(pu) \leq m^4 \sum_{u} \Pi_{i=1}^{*} \min \left( \frac{b_i^2}{m^2}, \frac{1}{4p^2u_i^2} \right)
\]

\[
\leq m^4 \sum_{j=0}^{4} \sum_{u} \Pi_{i=1}^{\mu} \frac{1}{4p^2u_i^2} \quad \text{if } \frac{u_i}{s_{\pi(i)}} \leq \frac{b_{\pi(i)}}{s_{\pi(i)}}, \\
\frac{b_i^2}{m^2} \quad \text{if } \frac{u_i}{s_{\pi(i)}} > \frac{b_{\pi(i)}}{s_{\pi(i)}}, \\
\text{otherwise}
\]

\[
\leq m^4 \sum_{j=0}^{4} \sum_{k_1=0}^{\infty} \cdots \sum_{k_j=0}^{\infty} \Pi_{i=1}^{\mu} \frac{b_i^2}{m^2} \sum_{k_1=0}^{\infty} \cdots \sum_{k_j=0}^{\infty} \Pi_{i=1}^{\mu} \frac{b_i^2}{m^2}
\]

\[
\leq m^{-4} |B|^2 \sum_{j=0}^{4} \sum_{k_1}^{\infty} \cdots \sum_{k_j}^{\infty} \Pi_{i=1}^{\mu} \sum_{k_1}^{\infty} \cdots \sum_{k_j}^{\infty} 1.
\]  

(15)

We break the sum over \( k_1, \ldots, k_j \) into two pieces \( S_1, S_2 \), the first being a sum over those \( k_i \) for which \( 2^{k_i} \leq 2^{-21} b_{\pi(i)} \), \( 1 \leq i \leq j \), and the second a sum over those \( k_i \) for which \( 2^{k_i} > 2^{-21} b_{\pi(i)} \), for some \( i \).

Now, in the sum \( S_1 \), \( 2^{k_i} q / b_{\pi(i)} \leq 2^{-21} q \), for \( 1 \leq i \leq j \) and \( q / b \ell \leq 2^{-21} q \) for all \( \ell \) (by (7)). Thus we can apply the upper bound (14) to the inner sum \( \sum_{i}^{u} \) in (15) to get,

\[
|S_1| \leq \sum_{k_1}^{\infty} \cdots \sum_{k_j}^{\infty} \left( \Pi_{i=1}^{\mu} \frac{1}{2^{k_i}} \right) \left( \frac{\alpha_{\pi(i)}}{q} \sum_{i=1}^{\mu} \left( \frac{2^{k_i+1} q}{b_{\pi(i)}} + 1 \right) \Pi_{\ell} \left( \frac{q}{b_{\ell}} + 1 \right) \right)
\]

\[
\leq \sum_{k_1}^{\infty} \cdots \sum_{k_j}^{\infty} \left( \Pi_{i=1}^{\mu} \frac{1}{2^{k_i}} \right) \left( \frac{\alpha_{\pi(i)}}{q} \sum_{i=1}^{\mu} \left( \frac{2^{k_i+2} q}{b_{\pi(i)}} \Pi_{b_{\pi(i)} > q} \frac{2^{k_i+2} q}{b_{\ell}} + \frac{2 q}{b_{\ell}} \Pi_{\ell} q + 2^{-14} q \right) \right)
\]

\[
\leq \frac{2^{2\beta+1} q^{s-1}}{\beta} \sum_{k_1}^{\infty} \cdots \sum_{k_j}^{\infty} \Pi_{i=1}^{\mu} \frac{1}{2^{k_i}} + 2^{-14} q \sum_{k_1}^{\infty} \cdots \sum_{k_j}^{\infty} \Pi_{i=1}^{\mu} \frac{1}{2^{k_i}},
\]

\[
\leq \frac{2^{2\beta+1} q^{s-1}}{\beta} + 2^{-14} q + q,
\]

where \( \beta \) and \( s \) are defined in (9). Inserting the lower bound for \( \beta \) given in (10) we obtain

\[
|S_1| \leq 2^{-13+2j} q.
\]  

(16)

In the sum \( S_2 \) we have \( 2^{k_i} > 2^{-21} b_{\pi(i)} \) for some \( i \) with \( 1 \leq i \leq j \). In particular \( k_i > 44 \) (by (7)). We consider just the case \( k_1 > 44 \), and multiply the result by \( j \). Applying the upper bound (13) to the inner sum in \( S_2 \) we obtain

\[
|S_2| \leq j \sum_{k_1=44}^{\infty} \sum_{k_0=0}^{\infty} \cdots \sum_{k_j=0}^{\infty} \left( \Pi_{i=1}^{j} \frac{1}{2^{k_i}} \right) 2^4 \left( \sum_{i=1}^{j} \left( \frac{2^{k_i+1} q}{b_{\pi(i)}} + 1 \right) \right) \Pi_{\ell} \left( \frac{q}{b_{\ell}} + 1 \right) + q
\]

\[
\leq 2^4 j \sum_{k_1=44}^{\infty} \cdots \sum_{k_j=0}^{\infty} \left( \Pi_{i=1}^{j} \frac{1}{2^{k_i}} \right) \left[ \frac{1}{q} \Pi_{b_{\pi(i)} \leq q} \frac{2^{k_i+2} q}{b_{\pi(i)}} \Pi_{b_{\pi(i)} > q} \frac{2 q}{b_{\ell}} \Pi_{\ell>q} \right]
\]

\[
\leq \frac{2^{2j+8} q^{s-1}}{\beta} \sum_{k_1=44}^{\infty} \cdots \sum_{k_j=0}^{\infty} \Pi_{i=1}^{j} \frac{1}{2^{k_i}} + 2^4 j q \sum_{k_1=44}^{\infty} \cdots \sum_{k_j=0}^{\infty} \Pi_{i=1}^{j} \frac{1}{2^{k_i}}
\]

\[
\leq j 2^{j-139} q + j 2^{j-84} q \leq 2^{-77} q,
\]  

(17)
where again we have used the lower bound for $\beta$ in (10). Thus by (15), (16) and (17) we have

$$
q^2|V_p| \sum_{Q^*(u)\equiv 0 \mod q} a(pu) \leq q^2 p^3 m^{-4} |B|^2 \sum_{j=0}^{4} \sum_{\pi} 2^{-12+2j} q^3
\leq \frac{5}{32} \frac{|B|^2}{m}.
$$

§6. The sum $\sum a(y)$.

Set $y = v + pu$. Then as $v$ and $u$ run through complete sets of residues mod $p$ and mod $q$ respectively with $|v_i| < \frac{p}{2}$ and $|u_i| < \frac{q}{2}$, $1 \leq i \leq 4$, $y$ runs through a complete set of residues mod $m$, with $|y_i| < \frac{m}{2}$, $1 \leq i \leq 4$. We also note that $|y_i| \geq |pu_i| - |v_i| > \frac{1}{2} p|u_i|$, if $|u_i| \neq 0$. Thus, by (11),

$$
\sum_{Q^*(y)\equiv 0 \mod p} a(y) \leq m^4 \sum_{y} \prod_{i=1}^{4} \min \left( \frac{b_i^2}{m^2}, \frac{1}{4y_i^2} \right)
\leq m^4 \sum_{y} \prod_{i=1}^{4} \sum_{u_i = -[q/2]}^{[q/2]} \min \left( \frac{b_i^2}{m^2}, \frac{1}{4(v_i + pu_i)^2} \right)
\leq m^4 \sum_{y} \prod_{i=1}^{4} \left[ \min \left( \frac{b_i^2}{m^2}, \frac{1}{4v_i^2} \right) + \sum_{0 < |u_i| \leq |v_i|} \frac{b_i^2}{m^2} + \sum_{|u_i| > |v_i|} \frac{1}{4u_i^2} \right].
$$

(18)

Now if $b_i \leq q$ then the sum in (18) within the brackets is bounded above by

$$
\frac{b_i q}{m^2} + \frac{2q b_i}{m^2} + \frac{4q b_i}{m^2} = \frac{7q b_i}{m^2}.
$$

If $b_i > q$ then $\frac{b_i}{m} > \frac{1}{p}$, so that $\frac{4}{p^2} < \frac{4b_i^2}{m^2}$. Also $\frac{4}{p^2} < \frac{1}{v_i^2}$. Thus the same sum is bounded above by

$$
\min \left( \frac{b_i^2}{m^2}, \frac{1}{4v_i^2} \right) + \frac{4}{p^2} \leq \min \left( \frac{5b_i^2}{m^2}, \frac{5}{4v_i^2} \right).
$$

Thus, continuing from (18) we have

$$
\sum_{y} a(y) \leq m^4 \sum_{v} \prod_{b_i \leq q} \frac{7q b_i}{m^2} \prod_{b_i > q} \min \left( \frac{5b_i^2}{m^2}, \frac{5}{4v_i^2} \right)
\leq 7^4 m^{4-2s} q^s \sum_{v} \prod_{b_i > q} \left( \frac{b_i^2}{m^2}, \frac{1}{4v_i^2} \right)
\leq 7^4 m^{4-2s} q^s \sum_{j=0}^{4} \sum_{k_1=0}^{\pi} \cdots \sum_{k_{j}=0}^{\pi} \sum_{k_{j+1}=0}^{\pi} \cdots \sum_{k_{j+s}=0}^{\pi} \prod_{b_{s+1} > q} \frac{b_{s+1}^2}{4k_1 m^2} \Pi_{b_i > q} \frac{b_i^2}{m^2}
\leq \frac{7^4 |B|^2 q^s}{m^4 \beta} \sum_{j=0}^{4} \sum_{k_1} \cdots \sum_{k_{j}} \Pi_{b_{s+1} > q} \frac{1}{4k_1} \sum_{v} \prod_{(above)}(19)
$$
Now, if \( b_{\pi(i)} \leq q \) for some \( i \), then \( \frac{m}{2b_{\pi(i)}} \geq \frac{p}{2} \) and so the sum over \( v \) in (19) is empty. Thus we may assume that \( b_{\pi(i)} > q \) for all \( i \). If \( b_t \leq q \) then we replace \( \frac{m}{2b_t} \) by \( \frac{p}{2} \) in the upper bound on \( |v| \) in (19). Then using the upper bound in (13) we have that the sum over \( v \) in (19) is bounded by

\[
\sum_{v_{\pi(i)} < \frac{2m}{2b(i)}, 1 \leq i \leq j} 1 \leq \frac{24}{p} \left( \Pi_{i=1}^{j} \frac{2^{k_i} + 2m}{b_{\pi(i)}} \right) \left( \Pi_{b_t > q} \frac{2m}{b_t} \right) p^s + 2^4 p
\]

\[
\leq \frac{2^{12} \beta p^{s-1} m^{4-s}}{|B|} \Pi_{i=1}^{j} 2^{k_i} + 2^4 p.
\]

Thus,

\[
\sum_{y} a(y) \leq \frac{2^{32} |B|}{p} + 2^{24} \frac{pq^4 |B|^2}{m^4 \beta}
\]

\[
\leq 2^{32} \frac{|B|}{p} + 2^{-79} \frac{pq^2}{m^4} |B|^2
\]

(\text{using (10)},

\[
\leq 2^{-71} \frac{|B|^2}{pm^2} + 2^{-79} \frac{|B|^2}{pm^2}
\]

\[
< 2^{-70} \frac{|B|^2}{pm^2},
\]

(\text{using (8)}), and so

\[
p^2 q \sum_{Q^*(y) \equiv 0 \bmod p} a(y) \leq 2^{-70} \frac{|B|^2}{m}.
\]

References

1. T. Cochrane, Small zeros of quadratic congruences modulo \( pq \), Mathematika 37, (1990), 261-272.


