Small Zeros of Quadratic Forms Modulo \( p \)

**TODD COCHRANE**

*Department of Mathematics, Kansas State University, Cardwell Hall, Manhattan, Kansas 66506*

*Communicated by P. T. Bateman*

Received March 14, 1988

Let \( Q(x) = Q(x_1, x_2, \ldots, x_n) \) be a quadratic form with integer coefficients and \( p \) be an odd prime. Suppose that \( n \) is even and \( \text{det} Q \not\equiv 0 \pmod{p} \). Set \( \Delta = \left( \frac{-1}{p} \right) \text{det} Q \), and let \( Q^*(x) \) be the form associated with the inverse of the matrix representing \( Q(x) \), \( \pmod{p} \). If \( \Delta = 1 \), it is known that there exists a nonzero \( x \) with \( \max |x_i| < p^{1/2} \) and \( Q(x) \equiv 0 \pmod{p} \). If \( \Delta = -1 \) we show here that there exists a nonzero \( x \) with \( \max |x_i| < p^{1/2} \) and either \( Q(x) \equiv 0 \pmod{p} \) or \( Q^*(x) \equiv 0 \pmod{p} \). We also show that for any form \( Q(x) \), if \( n > 4 \log_2 p + 3 \), then the congruence \( Q(x) \equiv 0 \pmod{p} \) has a solution with \( 0 < \max |x_i| < p^{1/2} \).

1. INTRODUCTION

Let \( Q(x) = Q(x_1, x_2, \ldots, x_n) \) be a quadratic form with integer coefficients and \( p \) be an odd prime. Set \( \|x\| = \max |x_i| \). Heath-Brown [3] has shown that for \( n \geq 4 \), the congruence

\[
Q(x) \equiv 0 \pmod{p}
\]

has a nonzero solution \( x \) with \( \|x\| \ll p^{1/2} \log p \). The smallest nonzero solution one can hope for (for a general \( Q \)) is one with \( \|x\| \ll p^{1/2} \), but it is unknown whether such a solution always exists.

When \( n \) is even one can use Minkowski's theorem from the geometry of numbers to obtain a nonzero solution of (1) of order \( p^{1/2} \), in certain cases. Set

\[
\Delta = \Delta_Q = \left( \frac{-1}{p} \right)^{n/2} \frac{\text{det} Q}{p}
\]

(Legendre symbol),

if \( p \nmid \text{det} Q \), and \( \Delta = 0 \) if \( p \mid \text{det} Q \). If \( \Delta = 0 \) or 1, then one obtains in this manner a solution of (1) with \( 0 < \|x\| < p^{1/2} \); see [3, Theorem 2] for the case \( n = 4 \), and [2, Lemma 3, Theorem 2].
If \( n \geq 4 \) is even and \( \Delta = -1 \) we are able to prove that either \( Q(x) \) or \( Q^*(x) \), the conjugate form associated with the inverse (mod \( p \)) of the matrix representing \( Q(x) \), has a zero \( x \) (mod \( p \)) with \( 0 < \|x\| \leq p^{1/2} \).

**Theorem 1.** If \( Q(x) \) is a quadratic form in an even number of variables \( n \geq 4 \) and \( \Delta_Q = -1 \), then there exists an \( x \in \mathbb{Z}^n \) such that \( 0 < \|x\| \leq p^{1/2} \) and either \( Q(x) \equiv 0 \) (mod \( p \)) or \( Q^*(x) \equiv 0 \) (mod \( p \)).

(The constant we obtain in the \( \ll \) inequality of the theorem depends on \( n \), but one may be able to refine our proof to get a constant independent of \( n \).)

This theorem is best possible, for if we consider the form \( Q(x) = x_1^2 + x_2^2 + \cdots + x_n^2 = Q^*(x) \), it is clear that any nonzero solution of (1) satisfies \( \|x\| \geq (1/\sqrt{n})p^{1/2} \). The proof of Theorem 1 follows the line of argument used in Heath-Brown's paper [3].

One particular consequence of Theorem 1 is that any self-conjugate quadratic form (mod \( p \)) in an even number of variables \( n \geq 4 \) has a nontrivial zero \( x \) with \( \|x\| \leq p^{1/2} \). Another special case where zeros of order \( p^{1/2} \) are obtained is given in:

**Theorem 2.** Suppose \( Q(x_1, x_2, x_3, x_4) \) can be expressed in the form

\[
Q(x_1, x_2, x_3, x_4) \equiv Q_1(x_1, x_2) + Q_2(x_3, x_4) \pmod{p},
\]

for some quadratic forms \( Q_1 \) and \( Q_2 \). Then there exists a nonzero \( 4 \)-tuple of integers \( x \) such that \( \|x\| < p^{1/2} \) and \( Q(x) \equiv 0 \) (mod \( p \)).

The proof of Theorem 2 is immediate. If \( \Delta_Q = -1 \), then either \( \Delta_{Q_1} = 1 \) or \( \Delta_{Q_2} = 1 \) and so the small solution can be obtained by setting \( x_3 = x_4 = 0 \) or \( x_1 = x_2 = 0 \). As a Corollary we obtain

**Theorem 3.** Suppose that \( n > 4 \log_2 p + 3 \). Then for any quadratic form \( Q(x) \) in \( n \) variables over \( \mathbb{Z} \) there exists a nonzero solution of (1) with \( \|x\| < p^{1/2} \).

We note that a slightly weaker form of Theorem 3 follows immediately from Theorem 1 of Schinzel, Schlickewei, and Schmidt [4]. They prove that (1) has a nonzero solution with \( \|x\| < p^{1/2} + 1/2(n - 1) \) for \( n \geq 3 \) (in fact, their result holds for composite moduli as well). If \( n \) satisfies the condition of Theorem 3 their bound simplifies to \( \|x\| < \sqrt{2}p^{1/2} \). Thus, our improvement is only in the constant in front of \( p^{1/2} \), but this theorem together with Theorem 2 and Theorem 2 of [3] leads us to ask whether we can always obtain a nonzero solution of (1) with \( \|x\| < p^{1/2} \).
2. Lemmas

To prove Theorem 1 we shall use finite Fourier series over $\mathbb{F}_p$, the finite field in $p$ elements. Henceforth we shall assume that $n$ is even, $p$ is an odd prime, and that $Q(x)$ is a nonsingular quadratic form in $\mathbb{F}_p[x_1, x_2, \ldots, x_n]$. Let $e_p(\alpha) = e^{2\pi i \alpha/p}$, $x \cdot y = \sum_{i=1}^{n} x_i y_i$, and $\sum_x = \sum_{x \in \mathbb{F}_p^n}$. Let $V = V_Q$ denote the set of zeros of $Q(x)$ in $\mathbb{F}_p^n$ and let $Q^*(x)$ and $\Delta = \Delta_Q$ be as defined above. For $y \in \mathbb{F}_p^n$, set

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

**Lemma 1.** Suppose that $n$ is even. Then for $y \in \mathbb{F}_p^n$,

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

The proof of Lemma 1 is given in Carlitz [1], and is implicit in Heath-Brown's paper [3] for the case $n = 4$.

Let $\alpha(x)$ be a real valued function defined on $\mathbb{F}_p^n$ with finite Fourier expansion $\alpha(x) = \sum_y a(y) e_p(x \cdot y)$, where $a(y) = p^{-n} \sum_x \alpha(x) e_p(-x \cdot y)$. Then by Lemma 1,

$$\sum_{x \in V} \alpha(x) = a(0) |V| + \sum_{y \neq 0} a(y) \phi(V, y)$$

$$= p^{-1} \sum_x \alpha(x) + \sum_y a(y) \phi(V, y)$$

$$= p^{-1} \sum_x \alpha(x) + \Delta(p-1) p^{n/2-1} \sum_{Q^*(y) = 0} a(y)$$

$$- \Delta p^{n/2-1} \sum_{Q^*(y) \neq 0} a(y),$$

and so we obtain

**Lemma 2.** For any $\alpha(x)$ as given above

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

Let $R = R(M_1, \ldots, M_n)$ be the box of points in $\mathbb{F}_p^n$ given by

$$B = \{ x \in \mathbb{F}_p^n : |x_i| \leq M_i, 1 \leq i \leq n \},$$

where $M_1, \ldots, M_n$ are positive integers less than $p/2$. (We have identified
Let $F_p$ with the set of integer representatives \( \{ x \in \mathbb{Z} : |x| < p/2 \} \). Let $\chi_B$ be the characteristic function of $B$ with Fourier expansion $\chi_B(x) = \sum_y a_B(y) e_p(x \cdot y)$. Then for $y \in F^n_p$,

$$a_B(y) = p^{-n} \prod_{i=1}^n \frac{\sin \pi m_i y_i/p}{\sin \pi y_i/p},$$

where $m_i = 2M_i + 1$, and a term in the product is defined to be $m_i$ if $y_i = 0$.

Set $\alpha(x) = \chi_B * \chi_B(x) \equiv \sum_u \chi_B(u) \chi_B(x - u)$. Then the Fourier coefficients of $\alpha(x)$ are given by $a(y) = p^n a_B^2(y)$.

If $\Delta_Q = -1$, then by Lemma 2 we have

\[
\sum_{x \in \mathcal{V}} \chi_B * \chi_B(x) = p^{-1} |B|^2 + p^{n/2 - 1} |B| - p^{(3/2)n} \sum_{Q^*(y) = 0} a_B^2(y)
\]

\[
< p^{-1} |B|^2 + p^{n/2 - 1} |B|. \tag{2}
\]

On the other hand,

\[
\sum_{x \in \mathcal{V}} \chi_B * \chi_B(x) \geq \sum_{x \in \mathcal{V} \cap B} 2^{-n} |B| = 2^{-n} |B| |B \cap \mathcal{V}|.
\]

Thus, we obtain

**Lemma 3.** If $\Delta_Q = -1$, then

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

(When $n = 4$, this is essentially Lemma 5 of [3], with an explicit constant given instead of a big $oh$.)

### 3. Proof of Theorem 1

Let $M < p/2$ be a positive integer, $B$ be the box $B(M, M, ..., M)$, $m = 2M + 1$ and $\alpha(x) = \chi_B * \chi_B(x)$. Suppose that $\Delta_Q = -1$, and let $D$ be a parameter such that $Q^*$ has no zero $y$ with $0 < \|y\| < D$. Then, letting $\pi$ run through the injections of $\{1, 2, ..., j\}$ into $\{1, 2, ..., n\}$, and letting $\Sigma^*$ be an abbreviation for $\Sigma_{y^*(y) = 0, y \neq 0}$, we have

\[
\sum^* a_B^2(y) = \sum^* a_B^2(y) = \sum_{|y| > D} \sum_{j=1}^n \sum_{|y^*(y)| \geq D} a_B^2(y)
\]

\[
= \sum_{j=1}^n \sum_{\pi} \sum_{k_1=1}^{\infty} \cdots \sum_{k_l=1}^{\infty} \sum_{D \leq |y| < D, \text{ otherwise}} a_B^2(y).
\]
Applying Lemma 3 to $Q^*$ and using the fact that

$$a^2_{\theta}(y) \leq \prod_{i=1}^{n} \min \left( \frac{m^2}{p^2}, \frac{1}{4y_i^2} \right),$$

we obtain

$$\sum_{y} a^2_{\theta}(y) \leq \sum_{j=1}^{n} \binom{n}{j} \sum_{k_1=1}^{\infty} \cdots \sum_{k_j=1}^{\infty} \left\{ \left( \frac{m}{p} \right)^{2(n-j)} \left( \frac{1}{4} \right) \prod_{i=1}^{j} \left( 2^{k_i-1}D \right)^{-2} \cdot 2^n 2^{k_1} \cdots + k_j(D+1)^n p^{-1} + p^{n/2-1} \right\}$$

$$= C_1 + C_2$$

say, where

$$C_1 = 2^{2n}(D+1)^n p^{-1} \sum_{j=1}^{n} \binom{n}{j} \left( \frac{m}{p} \right)^{2(n-j)} D^{-2j} \sum_{k_1=1}^{\infty} \cdots \sum_{k_j=1}^{\infty} \frac{1}{2^{k_1}} \cdots \frac{1}{2^{k_j}}$$

and

$$C_2 = 2^n p^{n/2-1} \sum_{j=1}^{n} \binom{n}{j} \left( \frac{m}{p} \right)^{2(n-j)} D^{-2j} \sum_{k_1=1}^{\infty} \cdots \sum_{k_j=1}^{\infty} \frac{1}{4^{k_1}} \cdots \frac{1}{4^{k_j}}$$

Then, by (2) and the observation that $\sum_{Q^*(y)} a^2_{\theta}(y) \leq a^2_{\theta}(0) + C_1 + C_2$, we deduce that

$$\sum_{x \in \mathcal{V}, x \neq 0} \chi_{B^*} \chi_{B}(x) \geq p^{-1} |B|^2 + (p^{n/2-1} |B| - |B| - p^{-n/2} |B|^2)$$

$$- p^{(3/2)n} C_1 - p^{(3/2)n} C_2. \quad (3)$$

Now, the quantity in the parentheses on the right-hand side of (3) is positive if $|B| < p^{n-1} - p^{n/2}$, and so the right-hand side of (3) is positive if the following three conditions hold,

$$|B| < p^{n-1} - p^{n/2}, \quad (4)$$

$$p^{-1} |B|^2 \geq 2C_1 p^{(3/2)n}, \quad (5)$$
and
\[ p^{-1} |B|^2 \geq 2C_2 p^{(3/2)n}. \]  
(6)

If these 3 conditions hold it follows that \( Q(x) \) has a zero \( x \) with \( 0 < \|x\| \leq 2M < m. \)

Set \( \lambda = p/mD \) and suppose that \( \lambda^2 < 1/2n. \) Then
\[ C_1 = 2^{2n}(D + 1)^n m^{2n} p^{-(2n+1)}[(1 + \lambda^2)^n - 1] \]
\[ \leq 2^{2n}(D + 1)^n m^{2n} p^{-(2n+1)2n\lambda^2}, \]
and
\[ C_2 \leq 2^n m^{2n} p^{-(3/2)n + 1/2n\lambda^2/3}. \]

Thus (6) is satisfied if \( \lambda^2 = 3/(2^{2+n}n). \) For this choice of \( \lambda, \) (5) holds true if \( D = (1/3^{1/2}) p^{1/2} - 2, \) and for this value of \( D, \) \( m = p/D\lambda \ll p^{1/2}. \)
(Inequality (4) holds trivially for \( m \ll p^{1/2} \) and \( p \) sufficiently large.)

4. PROOF OF THEOREM 3

Let \( Q(x) \in \mathbb{Z}[x_1, ..., x_n] \) be a quadratic form and \( p \) be an odd prime. By setting one variable equal to zero in case \( n \) is odd, we may assume that \( n \) is even and write
\[ Q(x) = a_{11}x_1^2 + a_{12}x_1x_2 + x_1L_1(x_3, x_5, ..., x_{n-1}) + x_1L_2(x_4, x_6, ..., x_n) \]
\[ + a_{22}x_2^2 + x_2L_3(x_3, x_5, ..., x_{n-1}) + x_2L_4(x_4, x_6, ..., x_n) \]
\[ + Q_1(x_3, x_4, ..., x_n), \]
for some linear forms \( L_1, L_2, L_3, L_4 \) and quadratic form \( Q_1. \)

Let \( x_3, x_5, ..., x_{n-1} \) take on the values 0 and 1 and consider the mapping
\( (x_3, x_5, ..., x_{n-1}) \rightarrow (L_1, L_3). \)

If \( 2^{n/2-1} > p^2 \) then two different points get mapped to the same ordered pair \( \pmod{p} \), and taking their difference yields a nonzero point \( (x_3, x_5, ..., x_{n-1}) \) such that \( x_j = 0, 1, \) or \(-1\) for \( j = 3, 5, ..., n-1 \) and
\[ L_1(x_3, ..., x_{n-1}) \equiv L_3(x_3, ..., x_{n-1}) \equiv 0 \pmod{p}. \]

Similarly, there exists a nonzero point \( (x_4, x_6, ..., x_n) \) such that \( x_j = 0, 1, \) or \(-1\) for \( j = 4, 6, ..., n \) and
\[ L_2(x_4, ..., x_n) \equiv L_4(x_4, ..., x_n) \equiv 0 \pmod{p}. \]

Without loss of generality we may assume that \( x_3 \neq 0 \) and \( x_4 \neq 0. \)
Set
\[ x_j = \alpha_j x_3 / \alpha_3, \quad \text{for} \quad j = 5, 7, \ldots, n - 1 \] (7)
\[ x_j = \alpha_j x_4 / \alpha_4, \quad \text{for} \quad j = 6, 8, \ldots, n. \]

Then \( L_1, L_2, L_3, L_4 \) are identically zero (mod \( p \)), and the congruence \( Q(x) \equiv 0 \pmod{p} \) becomes
\[ a_{11} x_1^2 + a_{12} x_1 x_2 + a_{22} x_2^2 + Q_2(x_3, x_4) \equiv 0 \pmod{p} \] (8)
for some quadratic form \( Q_2 \). By Theorem 2, (8) has a nonzero solution with \( |x_i| < p^{1/2}, \ 1 \leq i \leq 4 \). Then by (7), the original congruence \( Q(x) \equiv 0 \pmod{p} \) has a nonzero solution with \( \|x\| < p^{1/2} \).

REFERENCES