JOURNAL OF NUMBER THEORY **42**, 57–60 (1992)

Small Solutions to a Given Quadratic Form with a Variable Modulus

DAVID GRANT

Department of Mathematics, Campus Box 426, University of Colorado at Boulder, Boulder, Colorado 80309-0426

Communicated by H. Zassenhaus

Received June 4, 1990

For a positive definite integral quadratic form $Q(\mathbf{x})$ in at least 4 variables, we show that there is a constant $c = c(Q)$ so that for any $m > 0$, there is a non-zero integral vector $\mathbf{x} = (x_i)$ such that $Q(\mathbf{x}) \equiv 0 \bmod (m)$, and $\max |x_i| \leqslant c\sqrt{m}$.

Let $Q(\mathbf{x}) \in \mathbb{Z}[x_1, ..., x_r]$ be a quadratic form. For any vector $\mathbf{x} \in \mathbb{Z}^r$, let $\|\mathbf{x}\| = \max_{1 \leqslant i \leqslant r} |x_i|$ measure the size of $\mathbf{x}$. Over the past decade, several authors sought uniform bounds for the smallest solution to

$$Q(\mathbf{x}) \equiv 0 \bmod (m), \qquad \mathbf{x} \neq 0, \tag{1}$$

for some fixed modulus $m > 0$ as Q varies over all quadratic forms. Schinzel, Schlickewei, and Schmidt [5] showed that one can take $\|\mathbf{x}\| \leqslant m^{1/2 + 1/2(r-1)}$. Heath-Brown [4] showed that $\|\mathbf{x}\| \leqslant m^{1/2} \log m$ is guaranteed so long as m is a prime. Cochrane first extended Heath-Brown's result to the case when m is the product of 2 distinct primes [2], and then showed that when m is a prime, $\|\mathbf{x}\| < \max(2^{19}\sqrt{m},\ 2^{22}10^6)$ [3].

In this paper, we will turn the problem on its head, and find a bound for the smallest solution to (1) for a fixed form Q, and varying modulus m.

THEOREM. *Let $Q(\mathbf{x})$ be a positive definite integral quadratic form in $r \geqslant 4$ variables. Then there is a constant $c = c(Q)$, such that for every $m \geqslant 2$, there exists a non-zero vector $\mathbf{x} \in \mathbb{Z}^r$ with*

$$Q(\mathbf{x}) \equiv 0 \bmod (m),$$

and $\|\mathbf{x}\| \leqslant c\sqrt{m}$.

Remarks. (i) Setting j variables equal to zero gives a positive definite quadratic form in $r - j$ variables. It therefore suffices to prove the theorem

0022-314X/92 $5.00

when $r=4$. Since we would expect c to increase as we specialize variables, we will assume only that r is even.

(ii) We can assume that m is a squarefree number greater than 1. If $m=m_0^2$, then $x_1=m_0$, $x_i=0$ $(1<i\leqslant r)$ gives a solution with $c=1$. If $m=m_1m_0^2$, with $m_1>1$, then a solution $Q(\mathbf{x}')\equiv 0 \bmod(m_1)$ with $\|\mathbf{x}'\|\leqslant c\sqrt{m_1}$ gives the solution $Q(\mathbf{x})\equiv 0 \bmod(m)$ with $\mathbf{x}=m_0\mathbf{x}'$ and $\|\mathbf{x}\|\leqslant c\sqrt{m}$.

(iii) If we fix a constant κ, then we can assume that m is not divisible by any primes $p\leqslant\kappa$. Take m squarefree. Then $m=m_1m_2$ with $m_1=\prod_{p\mid m,\, p\leqslant\kappa,\, p\,\text{prime}} p$, and $m_2=\prod_{p\mid m,\, p>\kappa,\, p\,\text{prime}} p$. Suppose that $m_2>1$, and $Q(\mathbf{x}')\equiv 0 \bmod(m_2)$ with $\|\mathbf{x}'\|\leqslant c'\sqrt{m_2}$. Then taking $\mathbf{x}=m_1\mathbf{x}'$, and $c=c'c_0$ where $c_0=\prod_{p\leqslant\kappa,\, p\,\text{prime}} p^{1/2}$, implies that $Q(\mathbf{x})\equiv 0 \bmod(m)$ with $\|\mathbf{x}\|\leqslant c\sqrt{m}$. If $m_2=1$, then $x_i=m_1$ $(1\leqslant i\leqslant r)$ is a solution, so we need only be sure to set $c\geqslant c_0$.

(iv) If we take $\kappa\geqslant 2$, then we can assume m is odd as well. Then $Q(\mathbf{x})\equiv 0 \bmod(m)$ if and only if $2Q(\mathbf{x})\equiv 0 \bmod(m)$, so we might as well assume that Q is an *even* integral quadratic form; i.e., if we write $Q(\mathbf{x})=\sum_{i,j} a_{ij}x_ix_j={}^t\mathbf{x}A\mathbf{x}$ with $A=[a_{ij}]$ a symmetric matrix, then $a_{ii}\in 2\mathbb{Z}$, $a_{ij}\in\mathbb{Z}$. We say that A *represents* the quadratic form Q. Since Q is positive definite, all the eigenvalues of A are positive.

From now on we will assume that $Q(\mathbf{x})={}^t\mathbf{x}A\mathbf{x}$ is an even integral, positive definite quadratic form in $r=2k$, $k\geqslant 2$, variables. We let q be the level of A, that is, the least positive integer so that qA^{-1} is also the matrix of an even integral quadratic form.

A central object in the study of Q is its associated theta function $\Theta(z)$, which is defined by

$$\Theta(z)=\sum_{\mathbf{v}\in\mathbb{Z}^r} e^{\pi i\,{}^t\mathbf{v}A\mathbf{v}z}, \tag{2}$$

which is convergent for all complex $z\in\mathfrak{h}=\{x+iy\mid y>0\}$. Immediately we see that

$$\Theta(z)=\sum_{n\in\mathbb{Z}} r(Q,2n)\,e^{2\pi i n z},$$

where $r(Q,2n)=\#\{\mathbf{x}\in\mathbb{Z}^r\mid Q(\mathbf{x})=2n\}$. It is well known that $\Theta(z)$ is a modular form [1]. We will describe the situation precisely.

Let $(\frac{a}{p})$ denote the Legendre symbol of an integer a modulo an odd prime p. We can define a Dirichlet character $\chi \bmod q$ by setting

$$\chi(-1)=(-1)^k$$

$$\chi(p)=\left(\frac{(-1)^k\det A}{p}\right) \qquad \text{for } p \text{ an odd prime, } p\nmid q,$$

and

$$\chi(2) = 2^{-k} \sum_{\mathbf{v} \in (\mathbb{Z}/2\mathbb{Z})^k} e^{\pi i {}^t\mathbf{v} A \mathbf{v}/2} \qquad \text{if } q \text{ is odd.}$$

Let $\Gamma_0(q) = \{(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}) \in SL_2(\mathbb{Z}) \mid q \mid c\}$. Then $\Gamma_0(q)$ acts on $\mathfrak{h}$ by linear fractional transformations. Recall that $f(z)$ is a modular form of weight k and character χ for $\Gamma_0(q)$ if f is holomorphic on $\mathfrak{h}$ (and at the cusps gotten by compactifying $\Gamma_0(q)\backslash\mathfrak{h}$), and satisfies

$$f\left(\frac{az+b}{cz+d}\right) = \chi(d)(cz+d)^k f(z)$$

for all $(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}) \in \Gamma_0(q)$. The space of such forms is denoted by $M_k(\Gamma_0(q), \chi)$ and contains $\Theta(z)$ (see [1]). The $\mathbb{C}$-vector space $M_k(\Gamma_0(q), \chi)$ is finite dimensional, and every element has a Fourier expansion (at the cusp at infinity) of the form

$$\sum_{n \geqslant 0} \alpha_n q^n, \qquad \text{where} \quad q = e^{2\pi i z}.$$

Hence, there exists a constant $\kappa(k, q, \chi)$ such that if $\alpha_0 \neq 0$, then $\alpha_n \neq 0$ for some $0 < n \leqslant \kappa(k, q, \chi)$ (since $1 \notin M_k(\Gamma_0(n), \chi)$).

The theorem now follows from the following proposition.

PROPOSITION. *Let A be a matrix which represents an even integral, positive definite quadratic form of level q in $2k$ variables, $k \geqslant 2$. Let $\kappa = \max(\kappa(k, q, \chi), q, 2)$, and λ be the smallest eigenvalue of A. Then if $m = \prod_{i=1}^{j} p_i$, where the p_i are distinct primes greater than κ, then there is a non-zero vector $\mathbf{x} \in \mathbb{Z}^{2k}$ satisfying* (1), *such that*

$$\|\mathbf{x}\| \leqslant \sqrt{2\kappa/\lambda}\sqrt{m}.$$

Proof. Let T_p denote the pth-Hecke operator on $M_k(\Gamma_0(q), \chi)$. When p is prime $p \nmid q$, T_p applied to a form $f = \sum_{n \geqslant 0} \alpha_n q^n$ yields

$$T_p(f) = \sum_{n \geqslant 0} b_n q^n \in M_k(\Gamma_0(q), \chi),$$

where $b_n = \alpha_{pn} + \chi(p)\, p^{k-1} \alpha_{n/p}$, and $\alpha_{n/p}$ is taken to be 0 if $p \nmid n$. Let $\Theta(z) = \sum_{n \geqslant 0} \alpha_{0,n} q^n$ be as in (2), and set $T_{p_i} \cdots T_{p_1} \Theta(z) = \sum_{n \geqslant 0} \alpha_{i,n} q^n$. Then

$$T_{p_j} \cdots T_{p_1} \Theta(z) = \alpha_{j,0} + \sum_{n \geqslant 1} \alpha_{j,n} q^n.$$

Since $Q(0)=0$, we have $\alpha_{0,0}=r(Q,0)\neq 0$. Hence

$$\alpha_{j,0}=\prod_{i=1}^{j}(1+\chi(p_i)\,p_i^{k-1})\,\alpha_{0,0}\neq 0,$$

since $k>1$.

Therefore there exists a positive integer n, $0<n\leqslant\kappa$, such that $\alpha_{j,n}\neq 0$. We can solve recursively for $\alpha_{j,n}$ in terms of $\alpha_{0,i}$, $i\geqslant 0$.

Indeed

$$\alpha_{j,n}=\alpha_{j-1,p_jn}+\chi(p_j)\,p_j^{k-1}\alpha_{j-1,n/p_j}.$$

But $p_j>\kappa\geqslant n$, so $p_j\nmid n$, and

$$\alpha_{j,n}=\alpha_{j-1,p_jn}$$

Likewise $p_{j-1}>n$, so $p_{j-1}\nmid p_jn$, and

$$\alpha_{j,n}=\alpha_{j-2,p_{j-1}p_jn}.$$

Continuing inductively we get

$$0\neq\alpha_{j,n}=\alpha_{0,p_1\cdots p_jn}=\alpha_{0,mn}.$$

But $\alpha_{0,mn}=r(Q,2mn)\neq 0$, so there exists a vector $\mathbf{x}\in\mathbb{Z}^{2k}$, $\mathbf{x}\neq 0$, such that

$$Q(\mathbf{x})=2mn\leqslant 2\kappa m.$$

Since $x_i^2\leqslant Q(\mathbf{x})/\lambda$ for $1\leqslant i\leqslant 2k$, we have

$$|x_i|\leqslant\sqrt{2\kappa/\lambda}\,\sqrt{m}$$

and

$$\|\mathbf{x}\|\leqslant\sqrt{2\kappa/\lambda}\,\sqrt{m}.$$

References

1. A. N. Andrianov, Quadratic forms and Hecke operators, *Grundl. Math. Wiss.* **286** (1987).
2. T. Cochrane, "Small Zeros of Quadratic Congruences Modulo pq," preprint.
3. T. Cochrane, "Small Zeros of Quadratic Congruences Modulo p, III," preprint.
4. D. R. Heath-Brown, Small solutions of quadratic congruences, *Glasgow Math. J.* **27** (1985), 87–93.
5. A. Schinzel, H. P. Schlickewei, and W. M. Schmidt, Small solutions of quadratic congruences and small fractional parts of quadratic forms, *Acta Arith.* **37** (1980), 241–248.