ACTA ARITHMETICA
LXIII.3 (1993)

On representing the multiple of a number by a quadratic form

by

TODD COCHRANE (Manhattan, Kan.)

Let $Q(\mathbf{x}) = \sum_{i\le j} c_{ij}x_ix_j$ be a quadratic form in n variables with integral coefficients. Write $Q(\mathbf{x}) = \frac{1}{2}\mathbf{x}A\mathbf{x}^t$ where $A = [a_{ij}]$ is a symmetric $n\times n$ matrix with entries $a_{ii} = 2c_{ii}$ and $a_{ij} = c_{ij}$ for $i < j$. Set $d = d(Q) = \det A$. We say Q is *primitive* if the coefficients c_{ij} are relatively prime, and *nonsingular* if $d \ne 0$. This paper addresses the following problem: Given a positive integer m what is the smallest nonzero integer λ (in absolute value) such that λm is represented over $\mathbb{Z}$ by Q, that is,

$$Q(\mathbf{x}) = \lambda m \tag{1}$$

is solvable over $\mathbb{Z}$. Grant [6] has shown that for positive definite forms in $n \ge 4$ variables there exists a constant $c_0(Q)$, depending on Q, such that for any positive integer m (1) is solvable for some λ with $0 < \lambda < c_0(Q)$. We extend his result in our first theorem.

THEOREM 1. (i) *For any nonsingular quadratic form Q in $n \ge 3$ variables there exists a constant $c_1(Q)$, depending only on Q, such that for any positive integer m,* (1) *is solvable for some λ with $0 < |\lambda| < c_1(Q)$. (λ can be taken positive or negative if Q is indefinite.)*

(ii) *If $n = 2$ the same result holds true provided that for any odd prime p dividing m to an odd multiplicity either $p \mid d$ or $\left(\frac{-d}{p}\right) = 1$.*

We note that when $n = 2$, the condition given in part (ii) of the theorem is also a necessary condition, for if p is an odd prime dividing m to an odd multiplicity and $\left(\frac{-d}{p}\right) = -1$, then whenever $Q(\mathbf{x}) = \lambda m$ is solvable it follows that $p \mid \lambda$, and consequently $|\lambda| \ge p$.

COROLLARY. *Let $Q(\mathbf{x})$ be a quadratic form in $n \ge 3$ variables. Then for any positive integer m the congruence $Q(\mathbf{x}) \equiv 0 \pmod{m}$ has a nonzero solution $\mathbf{x}$ with $\max|x_i| \le c(Q)m^{1/2}$, where $c(Q)$ is a constant depending only on Q. The same result holds when $n = 2$ for any value of m satisfying the hypothesis of Theorem* 1(ii).

This Corollary generalizes the result of [6]. The Corollary is immediate from Theorem 1 in case Q is a definite form, but requires Lemma 2 for indefinite forms. Of course, the real interest is in obtaining the result of the Corollary with $c(Q)$ replaced by a constant depending only on n (for $n \geq 4$). There has been a lot of work in this direction; see Schinzel, Schlickewei and Schmidt [11], Heath-Brown [7], [8], Sander [10], and Cochrane [4], [5].

We now seek the best possible value of λ. When $m = 1$ the problem reduces to finding the minimum nonzero value of $|Q(\mathbf{x})|$ as $\mathbf{x}$ runs through $\mathbb{Z}^n$. It is well known (see e.g. [2, Lemma 3.1, p. 135]) that for $n \geq 1$ there exists a constant $k(n)$, depending only on n, such that if $Q(\mathbf{x})$ is nonsingular then there exists an integral $\mathbf{x}$ with $0 < |Q(\mathbf{x})| \leq k(n)|d|^{1/n}$. We are led to ask the following

Question. For $n \geq 4$ does there exist a constant $c(n)$ depending only on n such that if $Q(\mathbf{x})$ is a nonsingular form in n variables and m is any positive integer, then (1) is solvable for some nonzero λ with $|\lambda| < c(n)|d|^{1/n}$?

It suffices to consider the case of primitive quadratic forms, for if $Q = aQ_1$ with Q_1 primitive and $\mathbf{x}_0$ is such that $Q_1(\mathbf{x}_0) = \lambda_0 m$ with $0 < |\lambda_0| < c(n)|d(Q_1)|^{1/n}$, then $Q(\mathbf{x}_0) = (a\lambda_0)m$ and $0 < |a\lambda_0| < c(n)|d(Q)|^{1/n}$. This observation also indicates that one can do no better than $|d|^{1/n}$ for imprimitive forms. However, for primitive forms we can do better.

Theorem 2. *There exist constants $c_2(n)$, $c_3(Q)$ and $c_4(d)$ depending only on n, Q and d respectively such that for any nonsingular primitive quadratic form Q we have the following.*

(i) *If Q is indefinite and $n \geq 4$ then, for any $m > 0$, (1) is solvable for some λ with*

$$0 < \lambda < c_2(n) d_0^{1/(2(n-2))} \tag{2}$$

where d_0 is the odd part of $|d|$. (A value for $c_2(n)$ can be easily calculated from the proof given here.)

(ii) *If Q is definite, $n = 4$, $m = m_1 m_2^2$ with m_1 square free and $m_1 \geq c_4(d)$, or Q is definite, $n \geq 5$ and $m \geq c_3(Q)$ then the same bound (2) holds for m, with λ replaced by $-\lambda$ for negative definite forms. (The constants $c_3(Q)$ and $c_4(d)$ are those given in Lemmas 4 and 5 respectively.)*

The upper bound $d_0^{1/(2(n-2))}$ in (2) is easily seen to be best possible. Consider for example the form $Q(\mathbf{x}) = x_1^2 + x_2^2 + m^2(x_3^2 + \ldots + x_n^2)$ where m is a product of distinct odd primes p satisfying $\left(\frac{-1}{p}\right) = -1$. Then any nonzero solution of $Q(\mathbf{x}) = \lambda m$ must satisfy $m \mid \lambda$ and hence $|\lambda| \geq m = d_0^{1/(2(n-2))}$. This example also shows that the best one can hope for with $n = 3$ is

$\lambda \ll |d|^{1/2}$. Theorem 2 establishes an affirmative answer to the question above for indefinite forms in $n \geq 4$ variables. The question remains open for definite forms in general but the following theorem lends further support to an affirmative answer.

THEOREM 3. *Let $Q(\mathbf{x})$ be a positive definite form in an even number of variables and $m = m_1^2 m_2$ with m_2 positive and square free. Suppose that for each odd prime divisor p of m_2 either $p \mid d$ or $\left(\frac{(-1)^{n/2}d}{p}\right) = 1$. Then* (1) *is solvable for some λ with*

$$0 < \lambda \leq \frac{4}{(B_n(1))^{2/n}} d^{1/n}, \tag{3}$$

where $B_n(1)$ is the volume of a ball of radius 1 *in $\mathbb{R}^n$.*

Lemmas. The idea for the proofs of Theorems 1 and 2 is quite simple. We make use of classical results that imply that under appropriate conditions (1) is solvable over $\mathbb{Z}$ if it is solvable over every local ring $\mathbb{Z}_p$; see Lemmas 1, 3, 4 and 5. Thus our problem reduces to finding a small value of λ such that (1) is solvable everywhere locally and this just amounts to having λ divisible by certain primes dividing $d(Q)$ and satisfying certain quadratic residuacity conditions for other primes dividing $d(Q)$. Theorem 3 follows from Lemma 6 and a standard argument from the geometry of numbers.

LEMMA 1 [13, Theorem 52]. *Let q be a nonzero integer and Q be a nonsingular quadratic form in $n \geq 3$ variables. Then there exists a nonzero integer $k = k(q, Q)$ with $(k, q) = 1$ such that if $a \in \mathbb{Z}$ is such that $k^2 \mid a$, aQ is indefinite or positive definite, and $Q(\mathbf{x}) \equiv a \pmod{t}$ is solvable for all nonzero t, then $Q(\mathbf{x}) = a$ is solvable over $\mathbb{Z}$.*

LEMMA 2 (Watson [15]). *Let Q be a quadratic form that does not represent zero nontrivially over $\mathbb{Z}$. Then for any integer a represented by Q there is a representation $Q(\mathbf{x}) = a$ with $\max |x_i| \leq \gamma(Q)|a|^{1/2}$, where $\gamma(Q)$ is a constant depending only on Q.*

LEMMA 3 [2, Theorem 1.5, p. 131]. *Let Q be a nonsingular, indefinite form in $n \geq 4$ variables and $a \neq 0 \in \mathbb{Z}$. If a is represented by Q over all $\mathbb{Z}_p$, then a is represented by Q over $\mathbb{Z}$.* (Cassels's book [2] deals with quadratic forms with even coefficients c_{ij}, for $i \neq j$, but the result extends to general quadratic forms.)

LEMMA 4 (Tartakovskiĭ [12]). *For any positive definite quadratic form in $n \geq 5$ variables there is a constant $c_3(Q)$ depending only on Q such that for any integer $a > c_3(Q)$, if $Q(\mathbf{x}) \equiv a \pmod{t}$ is solvable for all nonzero t then $Q(\mathbf{x}) = a$ is solvable over $\mathbb{Z}$.*

Lemma 5 (Linnik, Malyshev [9]). *There exists a constant $c_4(d)$ such that for any positive definite quadratic form Q in $n = 4$ variables, with $d = d(Q)$, and any square free integer $a > c_4(d)$ such that $Q(\mathbf{x}) \equiv a \pmod{t}$ is solvable for all nonzero t, the equation $Q(\mathbf{x}) = a$ is solvable over $\mathbb{Z}$.*

Lemma 6 (Cochrane [3]). *Let $F(\mathbf{x})$ be a form of any degree over $\mathbb{Z}$ and $m = p_1 p_2 \ldots p_k$ be a product of distinct primes. Suppose that for $i = 1, 2, \ldots, k$ the congruence $F(\mathbf{x}) \equiv 0 \pmod{p_i}$ has a subspace of solutions of dimension d_i. Then there exists a lattice of solutions of the congruence $F(\mathbf{x}) \equiv 0 \pmod{m}$ of volume $\prod_{i=1}^{k} p_i^{n-d_i}$.*

Lemma 7. *For any primitive quadratic form Q over $\mathbb{Z}$ in $n \geq 2$ variables there exists an odd number a_0 such that for any $a \equiv a_0 \pmod{8}$ the equation $Q(\mathbf{x}) = a$ is solvable over $\mathbb{Z}_2$.*

Proof. Since Q is primitive it represents some odd number a_0 over $\mathbb{Z}$. Now if $a \equiv a_0 \pmod{8}$ then $a = a_0 b^2$ for some 2-adic integer b. Thus Q represents a over the 2-adic integers.

Proof of Theorem 1(i). We may assume that Q is primitive and that m is square free and relatively prime to $8d$ (see [6]). Since Q is primitive it represents some integer A (over $\mathbb{Z}$) relatively prime to $2d$. Then for any integer B with $B \equiv A \pmod{8d}$, it follows that Q represents B over every local ring $\mathbb{Z}_p$.

Let $k = k(q, Q)$ be as given in Lemma 1 with $q = 8d$. In particular, $(k, 8d) = 1$. Let β be such that $\beta k^2 m \equiv A \pmod{8d}$. Select β so that $0 < \beta < 8|d|$ if Q is indefinite or positive definite and $-8|d| < \beta < 0$ if Q is negative definite. Set $\lambda = \beta k^2$. Then $\lambda m Q$ is indefinite or positive definite, $k^2 \mid \lambda$, and $Q(\mathbf{x}) \equiv \lambda m \pmod{p^i}$ is solvable for all prime powers p^i. Thus, by Lemma 1, $Q(\mathbf{x}) = \lambda m$ is solvable over $\mathbb{Z}$, and $|\lambda| \leq 8|d|k^2$.

Proof of Theorem 1(ii). Again we may assume that m is an odd square free integer. For each prime $p \mid m$ the congruence $Q(\mathbf{x}) \equiv 0 \pmod{p}$ has a nonzero solution $\pmod{p}$ (since $p \mid d$ or $\left(\frac{-d}{p}\right) = 1$), and thus by Lemma 6 the congruence $Q(\mathbf{x}) \equiv 0 \pmod{m}$ has a lattice of solutions of volume m. Then by Minkowski's theorem there is a nonzero solution $\mathbf{x}$ of the congruence $Q(\mathbf{x}) \equiv 0 \pmod{m}$ with $\max |x_i| < m^{1/2}$. For this $\mathbf{x}$ we have $Q(\mathbf{x}) = \lambda m$ with $|\lambda| < |c_{11}| + |c_{12}| + |c_{22}|$. If $\lambda = 0$ then $Q(\mathbf{x})$ represents 0 over $\mathbb{Z}$ and we may assume without loss of generality that $Q(\mathbf{x}) = x_2(c_{12}x_1 + c_{22}x_2)$, with $c_{12} \neq 0$. In this case set $x_2 = m$, choose x_1 so that $0 < |c_{12}x_1 + c_{22}m| \leq |c_{12}|$ and set $\lambda' = c_{12}x_1 + c_{22}m$. Then $Q(\mathbf{x}) = \lambda' m$ with $0 < |\lambda'| \leq |c_{12}|$.

Proof of Corollary. If Q represents 0 nontrivially over $\mathbb{Z}$ the result is trivial, indeed one obtains a solution of $Q(\mathbf{x}) \equiv 0 \pmod{m}$ with $\max |x_i| \leq c(Q)$. Suppose now that Q does not represent 0 nontrivially.

In particular, Q is nonsingular. Let λ, m be such that $0 < |\lambda| < c_1(Q)$ and (1) is solvable. Then by Lemma 2 there exists an $\mathbf{x} \in \mathbb{Z}^n$ such that $Q(\mathbf{x}) = \lambda m$, with $0 < \max|x_i| \le \gamma(Q)(\lambda m)^{1/2}$. Thus $Q(\mathbf{x}) \equiv 0 \pmod{m}$ and $0 < \max|x_i| \le \gamma(Q)c_1(Q)^{1/2}m^{1/2}$. (If Q is definite one can be more precise and obtain $0 < \max|x_i| \le |\lambda/\beta|^{1/2}m^{1/2}$ where $|\beta|$ is the minimum modulus of the eigenvalues of Q.)

Proof of Theorem 2. Let Q be a nonsingular primitive quadratic form of determinant d and m be a positive integer. We may assume that m is odd and square free (for in general, if $m = m_1^2 2^e m_0$ with m_0 odd, square free, and $e = 0$ or 1, and λ is such that (2) holds and $Q(\mathbf{x}) = \lambda m_0$ for some $\mathbf{x} \in \mathbb{Z}^n$, then $Q(m_1 2^e \mathbf{x}) = 2^e \lambda m$). Now for any odd prime p, Q is equivalent over $\mathbb{Z}_p$ to one of the following types of forms:

(i) $\alpha_1 x_1^2 + \alpha_2 x_2^2 + \alpha_3 x_3^2 + Q'(x_4, \ldots, x_n)$,
(ii) $\alpha_1 x_1^2 + \alpha_2 x_2^2 + p\alpha_3 x_3^2 + p\alpha_4 x_4^2 + pQ'(x_5, \ldots, x_n)$, $p^{n-2} \mid d$,
(iii) $\alpha_1 x_1^2 + \alpha_2 x_2^2 + p\alpha_3 x_3^2 + p^2 Q'(x_4, \ldots, x_n)$, $p^{2n-5} \mid d$,
(iv) $\alpha_1 x_1^2 + \alpha_2 x_2^2 + p^2\alpha_3 x_3^2 + p^2 Q'(x_4, \ldots, x_n)$, $p^{2(n-2)} \mid d$,
(v) $\alpha_1 x_1^2 + \alpha_2 x_2^2 + p^3 Q'(x_3, \ldots, x_n)$, $p^{3(n-2)} \mid d$,
(vi) $\alpha_1 x_1^2 + p\alpha_2 x_2^2 + pQ'(x_3, \ldots, x_n)$, $p^{n-1} \mid d$,
(vii) $\alpha_1 x_1^2 + p^2\alpha_2 x_2^2 + p^2 Q'(x_3, \ldots, x_n)$, $p^{2(n-1)} \mid d$,
(viii) $\alpha_1 x_1^2 + p^j Q'(x_2, \ldots, x_n)$, $j \ge 3$, $p^{3(n-1)} \mid d$,

where α_1, α_2, α_3 are integers not divisible by p, and Q' is a quadratic form with integer coefficients. Next to each form we have put a power of p dividing d (not necessarily the largest power). Write

$$d = 2^e d_1 d_2 d_3 d_4 d_5 d_6 d_7 d_8\,,$$

where d_k consists of primes p such that Q is of type (k), $1 \le k \le 8$, and

$$m = m_1 m_2 m_3 m_4 m_5 m_6 m_7 m_8 m_9\,,$$

where $m_i \mid d_i$, $1 \le i \le 8$, and $(m_9, d) = 1$.

Our goal is to obtain a small value of λ such that $Q(\mathbf{x}) = \lambda m$ is solvable over $\mathbb{Z}_p$ for all p. By considering appropriate examples it is clear that λ must be divisible by $m_4 m_5 m_7 m_8$ in order to succeed in general, thus we consider instead the equation

$$Q(\mathbf{x}) = \lambda m_4 m_5 m_7 m_8 m = \lambda M, \tag{4}$$

say, where $M = m_4 m_5 m_7 m_8 m$. We consider in turn solving (4) over $\mathbb{Z}_p$ for the various odd primes p. For simplicity we shall assume that Q equals one of the eight canonical types given above (for a given prime p) and say that (4) is solvable if it is solvable over $\mathbb{Z}_p$.

(i) If $p\nmid d$ or $p\,|\,d_1$ (so that Q is of type (i)), then (4) is solvable for any λ.

(ii) If $p\,|\,d_2$ and $p\nmid m_2$ then (4) is solvable for any $\lambda\not\equiv 0 \pmod p$ (just put $x_3=\ldots=x_n=0$). If $p\,|\,m_2$, then we set $x_1=x_2=0$, and consider $\alpha_3x_3^2+\alpha_4x_4^2=\lambda M/p$, which again is solvable for any $\lambda\not\equiv 0 \pmod p$.

(iii) If $p\,|\,d_3$ and $p\nmid m_3$ then (4) is solvable for $\lambda\not\equiv 0 \pmod p$. If $p\,|\,m_3$, we set $x_1=x_2=0$ and are left with $\alpha_3x_3^2=\lambda M/p$, which is solvable provided $\left(\frac{\lambda}{p}\right)=\left(\frac{\alpha_3M/p}{p}\right)$.

(iv) If $p\,|\,d_4$ and $p\nmid m_4$ then (4) is solvable for $\lambda\not\equiv 0 \pmod p$. If $p\,|\,m_4$ then we set $x_1=py_1$, $x_2=py_2$ and consider $\alpha_1y_1^2+\alpha_2y_2^2+\alpha_3x_3^2=\lambda M/p^2$, which is solvable for any λ.

(v) If $p\,|\,d_5$ then as in (iv), (4) is solvable for any $\lambda\not\equiv 0 \pmod p$.

(vi) If $p\,|\,d_6$ and $p\nmid m_6$ then (4) is solvable provided $\left(\frac{\lambda}{p}\right)=\left(\frac{\alpha_1M}{p}\right)$. If $p\,|\,m_6$ then (4) is solvable provided $\left(\frac{\lambda}{p}\right)=\left(\frac{\alpha_2M/p}{p}\right)$.

(vii) If $p\,|\,d_7$ and $p\nmid m_7$ then (4) is solvable provided $\left(\frac{\lambda}{p}\right)=\left(\frac{\alpha_1M}{p}\right)$. If $p\,|\,m_7$ then we set $x_1=py_1$ and consider $\alpha_1y_1^2+\alpha_2x_2^2=\lambda M/p^2$, which is solvable for $\lambda\not\equiv 0 \pmod p$.

(viii) If $p\,|\,d_8$ and $p\nmid m_8$ then (4) is solvable provided $\left(\frac{\lambda}{p}\right)=\left(\frac{\alpha_1M}{p}\right)$. If $p\,|\,m_8$, then setting $x_1=py_1$ we see that (4) is solvable provided $\left(\frac{\lambda}{p}\right)=\left(\frac{\alpha_1M/p^2}{p}\right)$.

In summary, we see that (4) is solvable for all primes p (including $p=2$) if λ is such that

$$\lambda M\equiv a_0 \pmod 8\,, \tag{5}$$

$$\left(\frac{\lambda}{p}\right)=(-1)^{e_p}\quad \text{for } p\,|\,d_3d_6d_7d_8,\ p\nmid m_7\,, \tag{6}$$

and

$$p\nmid\lambda \quad \text{for } p\,|\,d_2d_4d_5m_7,\ p\nmid m_4 \tag{7}$$

where a_0 is the value given in Lemma 6, and the values e_p are as indicated above. Set

$$P=\prod_{\substack{p\,|\,d_3d_6d_7d_8\\ p\nmid m_7}} p \quad \text{(a product over distinct primes)}\,.$$

By standard arguments one can obtain a solution of (5), (6) and (7) with $\lambda\ll\sqrt{P}$, but lacking a convenient reference we have included an appendix to suit our particular needs. By Lemma 2 of the appendix there is a value of λ satisfying (5), (6) and (7) with

$$(8)\qquad 0<\lambda<\frac{32}{3}\pi^2\sqrt{P}\prod_{p\,|\,P}\frac{1+2/\sqrt{p}}{1-1/p}\prod_{\substack{p\,|\,d_2d_4d_5m_7\\ p\nmid m_4}}\frac{2-1/p}{1-1/p}.$$

Now, by the divisibility conditions given next to the canonical forms (i) to (viii) above we have

$$\prod_{p\,|\,d_2}p^{n-2}\prod_{p\,|\,d_3}p^{2n-5}\prod_{p\,|\,d_4}p^{2n-4}\prod_{p\,|\,d_5}p^{3n-6}\prod_{p\,|\,d_6}p^{n-1}\prod_{p\,|\,d_7}p^{2n-2}\prod_{p\,|\,d_8}p^{3n-3}\,\Big|\,d_0,$$

where d_0 is the odd part of d, and so

$$\begin{aligned}&\prod_{p\,|\,d_2}p^{1/2}\prod_{p\,|\,d_3}p^{(2n-5)/(2n-4)}\prod_{p\,|\,d_4}p\prod_{p\,|\,d_5}p^{3/2}\\&\times\prod_{p\,|\,d_6}p^{(n-1)/(2n-4)}\prod_{p\,|\,d_7}p^{(n-1)/(n-2)}\prod_{p\,|\,d_8}p^{(3n-3)/(2n-4)}\le d_0^{1/(2(n-2))}.\end{aligned}$$

Thus, by (4) and (8), the equation $Q(\mathbf{x})=\lambda m$ is solvable over $\mathbb{Z}_p$, for all primes p, for some λ with

$$\begin{aligned}0<\lambda&<\frac{32}{3}\pi^2m_4m_5m_7m_8\prod_{\substack{p\,|\,d_3d_6d_7d_8\\ p\nmid m_7}}p^{1/2}\frac{1+2/\sqrt{p}}{1-1/p}\prod_{\substack{p\,|\,d_2d_4d_5m_7\\ p\nmid m_4}}\frac{2-1/p}{1-1/p}\\&\le\frac{32}{3}\pi^2\prod_{p\,|\,d_2}\frac{2-1/p}{1-1/p}\prod_{p\,|\,d_3}p^{1/2}\frac{1+2/\sqrt{p}}{1-1/p}\prod_{p\,|\,d_4}p\prod_{p\,|\,d_5}p\frac{2-1/p}{1-1/p}\\&\quad\times\prod_{p\,|\,d_6}p^{1/2}\frac{1+2/\sqrt{p}}{1-1/p}\prod_{p\,|\,d_7}p\frac{2-1/p}{1-1/p}\prod_{p\,|\,d_8}p^{3/2}\frac{1+2/\sqrt{p}}{1-1/p}\\&\le c_2(n)d_0^{1/(2(n-2))},\end{aligned}$$

where $c_2(n)$ is an easily calculable constant depending only on n. Theorem 2 now follows from Lemmas 3, 4 and 5.

Proof of Theorem 3. Suppose first that m_2 is odd. Then for any prime divisor p of m_2 there exists a subspace of solutions of the congruence $Q(\mathbf{x})\equiv 0\pmod p$ of dimension $n/2$; see [3, Lemma 3]. Thus, by Lemma 6 there exists a lattice $\mathcal{L}$ of solutions of the congruence $Q(\mathbf{x})\equiv 0\pmod{m_2}$ of volume $m_2^{n/2}$. Let $\mathcal{R}$ be the convex region in $\mathbb{R}^n$ defined by $Q(\mathbf{x})\le r^2$. Then the volume of $\mathcal{R}$ is $2^{n/2}r^nB_n(1)/\sqrt{d}$ where $B_n(1)$ is the volume of an n-ball of radius 1. By Minkowski's theorem $\mathcal{R}$ contains a nonzero point $\mathbf{x}$ of $\mathcal{L}$ if $r^2\ge 2d^{1/n}m_2/B_n(1)^{2/n}$. Thus $Q(\mathbf{x})=\lambda m_2$ with $0<\lambda<2d^{1/n}/B_n(1)^{2/n}$, and $Q(m_1\mathbf{x})=\lambda m$. If m_2 is even, say $m_2=2m_3$, and $\mathbf{x}$ satisfies $Q(\mathbf{x})=\lambda m_3$ with λ as above, then $Q(2\mathbf{x})=(2\lambda)m_2$ and $Q(2m_1\mathbf{x})=(2\lambda)m$, with 2λ satisfying (3).

Note. If the odd square free part of m is relatively prime to d then the value $d_0^{1/(2(n-2))}$ in (2) can be replaced by

$$d_0^{1/(2(n-1))}\prod_{p\mid d_0}\frac{1+2/\sqrt{p}}{1-1/p}\,.$$

In particular, taking m to be one we conclude that for any indefinite, primitive nonsingular quadratic form Q in $n\ge 4$ variables there exists an $\mathbf{x}\in\mathbb{Z}^n$ such that

$$0<Q(\mathbf{x})<c_4(n)d_0^{1/(2(n-1))}\prod_{p\mid d_0}\frac{1+2/\sqrt{p}}{1-1/p}\,.$$

Watson [14] had shown earlier that for such forms in $n\ge 3$ variables an $\mathbf{x}$ exists with

$$0<Q(\mathbf{x})<c(\varepsilon)|d|^{1/(2(n-1))+\varepsilon}\,.$$

Appendix

Lemma 1. *Let n be any integer and m be a square free product of odd primes. Then*

$$\Big|\sum_{\substack{x=0\\(x,8m)=1}}^{8m-1}e^{2\pi i n x^2/(8m)}\Big|\le 4\prod_{\substack{p\mid m\\p\nmid n}}(1+\sqrt{p})\prod_{\substack{p\mid m\\p\mid n}}(p-1)\,.$$

Proof. Say $m=p_1p_2\dots p_k$ and set

$$x=x_1\frac{8m}{p_1}+x_2\frac{8m}{p_2}+\dots+x_k\frac{8m}{p_k}+x_{k+1}m$$

where x_i runs through $1,2,\dots,p_i-1$ for $1\le i\le k$ and x_{k+1} runs through $1,3,5,7$. Then

$$\begin{aligned}&\Big|\sum_{\substack{x=0\\(x,8m)=1}}^{8m-1}e^{2\pi i n x^2/(8m)}\Big|\\&=\Big|\sum_{x_1}\dots\sum_{x_{k+1}}\exp\Big(\frac{2\pi i n}{8m}\Big(x_1^2\frac{64m^2}{p_1^2}+\dots+x_k^2\frac{64m^2}{p_k^2}+x_{k+1}^2m^2\Big)\Big)\Big|\\&\le 4\prod_{i=1}^{k}\Big|\sum_{x_i}\exp\Big(\frac{2\pi i n(8m/p_i)x_i^2}{p_i}\Big)\Big|\le 4\prod_{p_i\mid n}(p_i-1)\prod_{p_i\nmid n}(1+\sqrt{p_i})\,.\end{aligned}$$

Lemma 2. *Let $D=8d_1d_2$ where d_1, d_2 are square free products of odd primes with $(d_1,d_2)=1$. Let c be any integer with $(c,D)=1$. Then there* *exists a* $\lambda \in \mathbb{Z}$ *with* $(\lambda, D) = 1$ *and*

$$0 < \lambda \le \frac{32}{3}\pi^2\sqrt{d_1}\prod_{p\,|\,d_1}\frac{1+2/\sqrt{p}}{1-1/p}\prod_{p\,|\,d_2}\frac{2-1/p}{1-1/p} \tag{1}$$

such that $cz^2 \equiv \lambda \pmod{8d_1}$ *for some* z *with* $(z, 8d_1) = 1$.

Proof. Write $x = 8d_1w + kd_2z^2$ where k is any integer satisfying $d_2k \equiv c \pmod{8d_1}$, w is such that $(w, d_2) = 1$ and z is such that $(z, 8d_1) = 1$. Then $x \equiv cz^2 \pmod{8d_1}$ and $(x, D) = 1$. Thus our goal is to find w, z such that x is small $\pmod{D}$. Let $I = \{0, 1, 2, \ldots, M-1\}$ where $M \in \mathbb{Z}$, $M < D$, let χ_I be the characteristic function of $I \pmod{D}$ and $\alpha = \chi_I * \chi_I$. Then α has a Fourier expansion

$$\alpha(x) = \sum_{y=-4d_1d_2+1}^{4d_1d_2} a(y)e_D(xy), \qquad \text{where } e_D(\ ) = e^{2\pi i(\ )/D},$$

and for $y \ne 0$,

$$|a(y)| = \frac{1}{D}\frac{\sin^2(\pi My/D)}{\sin^2(\pi y/D)}\,.$$

In particular, for $|y| \le 4d_1d_2$ we have

$$|a(y)| \le M^2/D \tag{2}$$

and

$$|a(y)| \le D/(4y^2) \qquad \text{for } y \ne 0\,. \tag{3}$$

Our goal is to show the following sum is positive for M sufficiently large:

$$\begin{aligned}
\sum_{\substack{w=1\\(w,d_2)=1}}^{d_2}\ \sum_{\substack{z=1\\(z,8d_1)=1}}^{8d_1} &\alpha(8d_1w + kd_2z^2)\\
&= \sum_{\substack{w=1\\(w,d_2)=1}}^{d_2}\ \sum_{\substack{z=1\\(z,8d_1)=1}}^{8d_1}\ \sum_{y} a(y)e_D((8d_1w + kd_2z^2)y)\\
&= a(0)\phi(8d_1d_2) + \sum_{y\ne 0} a(y)\sum_{w}\sum_{z} e_D(8d_1yw)e_D(kd_2yz^2)\\
&= a(0)\phi(8d_1d_2) + \text{Error}, \quad \text{say.}
\end{aligned}$$

To estimate the error term we first observe that if $\delta_2 = (d_2, y)$ then

$$\sum_{\substack{w=1\\(w,d_2)=1}}^{d_2} e_{d_2}(yw) = \sum_{\delta\mid\delta_2}\mu\left(\frac{d_2}{\delta}\right)\delta = \mu\left(\frac{d_2}{\delta_2}\right)\sum_{\delta\mid\delta_2}\mu\left(\frac{\delta_2}{\delta}\right)\delta$$
$$= \mu\left(\frac{d_2}{\delta}\right)\phi(\delta_2)\,.$$

Thus by Lemma 1 we have

$$|\mathrm{Error}| \le \sum_{\delta_1\mid 8d_1}\sum_{\delta_2\mid d_2}\sum_{\substack{y\ne 0\\(y,8d_1)=\delta_1\\(y,d_2)=\delta_2}} |a(y)|\Big|\sum_w e_{d_2}(yw)\Big|\Big|\sum_z e_{8d_1}(kyz^2)\Big|$$
$$\le 4\sum_{\delta_1\mid 8d_1}\sum_{\delta_2\mid d_2}\phi(\delta_2)\prod_{\substack{p\mid d_1\\p\mid\delta_1}}(p-1)\prod_{\substack{p\mid d_1\\p\nmid\delta_1}}(1+\sqrt{p})\sum_{\substack{y\ne 0\\(y,8d_1)=\delta_1\\(y,d_2)=\delta_2}}|a(y)|\,.$$

Set

$$y=\delta_1\delta_2\gamma \quad\text{ with }\quad \gamma=-\left[\frac{4d_1d_2}{\delta_1\delta_2}\right]+1,\ldots,\left[\frac{4d_1d_2}{\delta_1\delta_2}\right],\ \gamma\ne 0\,.$$

We split the sum over y into two pieces. Suppose first that $\delta_1\delta_2\le 2d_1d_2/M$. Then, using (2) and (3) we have

$$\sum_\gamma |a(\delta_1\delta_2\gamma)| = \sum_{|\gamma|\le\left[\frac{4d_1d_2}{\delta_1\delta_2 M}\right]}\frac{M^2}{D} + \sum_{|\gamma|\ge\left[\frac{4d_1d_2}{\delta_1\delta_2 M}\right]+1}\frac{D}{4(\delta_1\delta_2)^2\gamma^2}\,.$$

Now

$$\sum_{\gamma=N+1}^{\infty}\frac{1}{\gamma^2}\le\int_N^\infty\frac{1}{x^2}dx=\frac{1}{N}\qquad\text{for } N\ge 1\,,$$

and

$$\left[\frac{4d_1d_2}{\delta_1\delta_2M}\right]\ge\frac{4d_1d_2}{\delta_1\delta_2M}-1\ge\frac{2d_1d_2}{\delta_1\delta_2M}\qquad\text{for } \delta_1\delta_2<\frac{2d_1d_2}{M}\,.$$

Thus,

$$\sum_\gamma|a(\delta_1\delta_2\gamma)|\le 2\frac{M^2}{D}\cdot\frac{4d_1d_2}{\delta_1\delta_2M}+2\frac{D}{4(\delta_1\delta_2)^2}\cdot\frac{\delta_1\delta_2M}{2d_1d_2}=\frac{3M}{\delta_1\delta_2}\,.$$

Suppose now that $\delta_1\delta_2\ge 2d_1d_2/M$. Then

$$\sum_\gamma|a(\delta_1\delta_2\gamma)|<\frac{2d_1d_2}{(\delta_1\delta_2)^2}\sum_{|\gamma|\ge 1}\frac{1}{\gamma^2}\le\frac{M}{\delta_1\delta_2}\,\frac{\pi^2}{3}\,.$$

Thus for any choice of δ_1, δ_2 we have

$$\sum_{\substack{y\neq 0\\ (y,8d_1)=\delta_1\\ (y,d_2)=\delta_2}} |a(y)| < \frac{\pi^2}{3}\,\frac{M}{\delta_1\delta_2}\,,$$

and so,

$$\begin{aligned}|\mathrm{Error}| &< \frac{4}{3}\pi^2 M\Big[\sum_{\delta_1\,|\,8d_1}\frac{1}{\delta_1}\prod_{\substack{p\,|\,d_1\\ p\,|\,\delta_1}}(p-1)\prod_{\substack{p\,|\,d_1\\ p\,\nmid\,\delta_1}}(1+\sqrt{p})\Big]\Big(\sum_{\delta_2\,|\,d_2}\frac{\phi(\delta_2)}{\delta_2}\Big)\\ &< \frac{4}{3}\pi^2 M 2\prod_{p\,|\,d_1}(2+\sqrt{p})\prod_{p\,|\,d_2}\Big(2-\frac{1}{p}\Big).\end{aligned}$$

Now, the sum of interest is positive provided that

$$M^2\cdot\frac{1}{2}\prod_{p\,|\,d_1d_2}\Big(1-\frac{1}{p}\Big) > |\mathrm{Error}|\,.$$

It suffices to take

$$M \geq \frac{16}{3}\pi^2\prod_{p\,|\,d_1}\frac{2+\sqrt{p}}{1-1/p}\prod_{p\,|\,d_2}\frac{2-1/p}{1-1/p}\,,$$

whence (1) is obtained.

References

[1] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York 1966.

[2] J. W. S. Cassels, *Rational Quadratic Forms*, Academic Press, New York 1978.

[3] T. Cochrane, *Small solutions of congruences over algebraic number fields*, Illinois J. Math. 31 (1987), 618–625.

[4] —, *Small zeros of quadratic congruences modulo pq*, Mathematika 37 (1990), 261–272.

[5] —, *Small zeros of quadratic forms modulo p, III*, J. Number Theory 37 (1) (1991), 92–99.

[6] D. Grant, *Small solutions to a given quadratic form with a variable modulus*, to be published.

[7] D. R. Heath-Brown, *Small solutions of quadratic congruences*, Glasgow Math. J. 27 (1985), 87–93.

[8] —, *Small solutions of quadratic congruences, II*, Mathematika 38 (1991), 264–284.

[9] Yu. V. Linnik and A. V. Malyshev, *An elementary proof of the Kloosterman–Tartakovskiĭ theorem on the representations of numbers by positive quadratic forms*, in: Proc. Fourth All-Union Math. Congr., Leningrad 1961, Vol. II, Nauka, Leningrad 1964, 116–117.

[10] J. W. Sander, *A reciprocity formula for quadratic forms*, Monatsh. Math. 104 (1987), 125-132.

[11] 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.

[12] W. A. Tartakowsky [V. A. Tartakovskiĭ], *La détermination de la totalité des nombres représentables par une forme quadratique à plus de quatre variables*, C. R. Acad. Sci. Paris 186 (1928), 1337–1340, 1401–1403, 1684–1687. Errata to second paper: 187 (1928), 155.

[13] G. L. Watson, *Integral Quadratic Forms*, Cambridge University Press, London 1960.

[14] —, *The minimum of an indefinite quadratic form with integral coefficients*, J. London Math. Soc. 32 (1957), 503–507.

[15] —, *Bounded representations of integers by quadratic forms*, Mathematika 4 (1957), 17–24.

DEPARTMENT OF MATHEMATICS
KANSAS STATE UNIVERSITY
MANHATTAN, KANSAS 66506-2602
U.S.A.
E-mail: COCHRANE@KSUVM.BITNET

Received on 23.11.1990
and in revised form on 16.6.1992 (2098)