TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 291, Number 1, September 1985

SMALL ZEROS OF QUADRATIC FORMS[1]

BY
WOLFGANG M. SCHMIDT

ABSTRACT. We give upper and lower bounds for zeros of quadratic forms in the rational, real and p-adic fields. For example, given $r > 0$, $s > 0$, there are infinitely many forms $\mathfrak{F}$ with integer coefficients in $r + s$ variables of the type (r, s) (i.e., equivalent over $\mathbf{R}$ to $X_1^2 + \cdots + X_r^2 - X_{r+1}^2 - \cdots - X_{r+s}^2$) such that every nontrivial integer zero $\mathbf{x}$ has $|\mathbf{x}| \gg F^{r/2s}$, where F is the maximum modulus of the coefficients of $\mathfrak{F}$.

1. Introduction.

Let

$$\mathfrak{F}(\mathbf{X}) = \sum_{i,j=1}^{n} f_{ij} X_i X_j \neq 0$$

be a quadratic form with rational integer coefficients. We shall assume here and throughout that $f_{ij} = f_{ji}$. It had been shown by Cassels [**1**] that if $\mathfrak{F}$ has an integer zero $\mathbf{x} \neq \mathbf{0}$, then in fact it has an integer zero $\mathbf{x} \neq \mathbf{0}$ with

$$|\mathbf{x}| \ll F^{(n-1)/2}. \tag{1.1}$$

Here $|\mathbf{x}| = \max(|x_1|, \ldots, |x_n|)$, F is the maximum modulus of the coefficients f_{ij} and the constant in $\ll$ depends only on n. An example of Kneser (see [**2**]) shows that this is essentially best possible: given $n > 1$, there are infinitely many forms as above which do have nontrivial integer zeros, and every such zero has $|\mathbf{x}| \gg F^{(n-1)/2}$.

Recently Schlickewei [**3**] strengthened Cassel's result as follows. Suppose now that $\mathfrak{F}$ is of the type (r, s), i.e., $r + s = n$ and $\mathfrak{F}$ is equivalent over the reals to $X_1^2 + \cdots + X_r^2 - Y_1^2 - \cdots - Y_s^2$. We will assume that $r \geq s > 0$ and $n = r + s \geq 5$. Then $\mathfrak{F}$ certainly has an integer zero $\mathbf{x} \neq \mathbf{0}$ by Meyer's Theorem. Put

$$\alpha = \alpha(r, s) = \begin{cases} \frac{1}{2}(r/s) & \text{when } r \geq s + 3, \\ \frac{1}{2}(s + 2)/(s - 1) & \text{when } r = s + 2 \text{ or } s + 1, \\ \frac{1}{2}(s + 1)/(s - 2) & \text{when } r = s. \end{cases}$$

Then according to Schlickewei, $\mathfrak{F}$ has an integer zero $\mathbf{x} \neq \mathbf{0}$ with

$$|\mathbf{x}| \ll F^{\alpha}. \tag{1.2}$$

In the opposite direction, Watson [**6**] had constructed forms of the type (r, s) all of whose nontrivial integer zeros satisfied $|\mathbf{x}| \gg F^{(1/2)h}$ with $h = [r/s]$, i.e., the integer part of r/s. In the case when $r = n - 1$, $s = 1$, Watson's example becomes that of Kneser mentioned above.

Received by the editors April 30, 1984.
1980 *Mathematics Subject Classification.* Primary 10C05, 10E25; Secondary 10E99, 10C20.
[1]Written with partial support from NSF grant MCS-8211461.

We first wish to improve upon Watson's result. Given a point $\mathbf{x} = (x_1, \dots, x_n) \neq \mathbf{0}$ with real or complex components, put

$$\langle \mathbf{x} \rangle = \min_{x_i \neq 0} (|x_i|) \quad \text{and} \quad q(\mathbf{x}) = |\mathbf{x}| / \langle \mathbf{x} \rangle.$$

In other words $q(\mathbf{x})$ is the maximum quotient $|x_i|/|x_j|$ over i, j with $x_j \neq 0$.

THEOREM 1. *Suppose $n = r + s$, $r > 0$, $s > 0$. Given $C \geq 1$ there is a quadratic form $\mathfrak{F}$ with integer coefficients of the type (r, s) and with $F \leq C$, such that every point $\mathbf{x} \in \mathbf{R}^n \backslash \mathbf{0}$ with $\mathfrak{F}(\mathbf{x}) \leq 0$ has $q(\mathbf{x}) \gg C^{r/2s}$.*

In particular, $q(\mathbf{x}) \gg F^{r/2s}$. Thus every nontrivial *integer* zero has

$$|\mathbf{x}| \gg F^{r/2s}. \tag{1.3}$$

Therefore Watson's exponent $\frac{1}{2}[r/s]$ is improved to $\frac{1}{2}(r/s)$; this seemingly small improvement is rather nontrivial. When $r \geq s + 3$, the estimates (1.2), (1.3) complement each other, so that each is best possible.

Given a point $\mathbf{x} = (x_1, \dots, x_n)$ with coordinates in the p-adic field $\mathbf{Q}_p$ put $q_p(\mathbf{x}) = |\mathbf{x}|_p / \langle \mathbf{x} \rangle_p$, where

$$|\mathbf{x}|_p = \max(|x_1|_p, \dots, |x_n|_p), \qquad \langle \mathbf{x} \rangle_p = \min_{x_i \neq 0} |x_i|_p$$

and where $|\cdots|_p$ denotes the p-adic absolute value.

THEOREM 2. *Suppose $n \geq 5$ and a prime p are given. For each $C \geq 1$ there is a nondegenerate quadratic form $\mathfrak{F}$ with rational integer coefficients and with $F \leq C$, where F is defined as above in terms of the standard absolute value, such that every nontrivial p-adic zero $\mathbf{x}$ has*

$$q_p(\mathbf{x}) \gg C^{2/(n-4)},$$

with a constant in $\gg$ which depends only on n and p. Moreover, $\mathfrak{F}$ may be chosen of prescribed type (r, s) with $r + s = n$.

A point $\mathbf{x} \in \mathbf{Z}^n \backslash \mathbf{0}$ has $|\mathbf{x}| \geq q_p(\mathbf{x})$. Thus every nontrivial rational integer zero $\mathbf{x}$ of $\mathfrak{F}$ has

$$|\mathbf{x}| \gg C^{2/(n-4)} \geq F^{2/(n-4)}. \tag{1.4}$$

Of particular interest is the case $n = 5$, in which case we get $|\mathbf{x}| \gg F^2$. This holds in particular for forms of the type $(3, 2)$; the best lower bound in this case had been $|\mathbf{x}| \gg F^{3/2}$, due to Watson [**6**, last formula]. For the type $(3, 2)$ the estimates (1.2) and (1.4) complement each other and are therefore essentially best possible. In all the other cases when $r = s + 2$ or $s + 1$ or s, the question of the best possible exponent remains open.

The lower bounds given in Theorems 1 and 2 involve the real field and the p-adic fields. Our next theorems provide upper bounds for solutions in these fields. At least in the real case it seems natural to give bounds in terms of the eigenvalues of the coefficient matrix.

THEOREM 3. *Let $\mathfrak{F}(\mathbf{X})$ be a nonsingular quadratic form with real coefficients of the type (r,s) with $r>0$, $s>0$, $n=r+s\geq 3$. Let the eigenvalues of $\mathfrak{F}$ be*

$$\lambda_1 \geq \cdots \geq \lambda_r > -\mu_s \geq \cdots \geq -\mu_1$$

with positive λ_i, μ_j. Suppose that $\lambda_1 \geq \mu_1$, and put[2]

$$\nu = \begin{cases} \mu_1 & \text{if } r \geq 2 \text{ and } \lambda_2 \geq \mu_1, \\ \lambda_2 & \text{if } r \geq 2 \text{ and } \mu_1 > \lambda_2 \geq \mu_2, \\ \mu_2 & \text{if } r = 1 \text{ or if } r = 2 \text{ and } \mu_2 > \lambda_2. \end{cases} \tag{1.5}$$

Then $\mathfrak{F}$ has a real zero $\mathbf{x}$ with nonzero components and with

$$q(\mathbf{x}) \ll (\lambda_1/\nu)^{1/2}. \tag{1.6}$$

The constant in $\ll$ depends only on n. Since the components of $\mathbf{x}$ are nonzero, (1.6) may be rewritten as

$$|x_i| \gg (\nu/\lambda_1)^{1/2}|\mathbf{x}| \qquad (i=1,\ldots,n). \tag{1.7}$$

There is of course an analogous result when $\mu_1 \geq \lambda_1$.

Suppose now that $\mathfrak{F}$ has coefficients in $\mathbf{Z}$. Then all the eigenvalues are of modulus $\ll F$. Furthermore, $1 \leq \lambda_1 \cdots \lambda_r \mu_1 \cdots \mu_s \leq \lambda_1^r \mu_1^s \ll F^r \mu_1^s$, so that $\mu_1 \gg F^{-r/s}$. When $r \geq s$ and $\lambda_1 \geq \mu_1$, we have thus $\nu \gg F^{-r/s}$, at least in the first of the three cases in (1.5). But in the second and third cases one easily gets $\nu \gg F^{-2/(n-2)} \gg F^{-r/s}$ since $r \geq s$ and $n \geq 3$. Hence by Theorem 3 there is a real zero $\mathbf{x} \neq \mathbf{0}$ with

$$q(\mathbf{x}) \ll F^{(r/2s)+1/2}. \tag{1.8}$$

The same conclusion may be drawn when $r \geq s$ and $\mu_1 \geq \lambda_1$. But this consequence of Theorem 3 is rather weak as compared to (1.2). According to (1.2) we may for $r \geq s+3$ get an $\mathbf{x}$ with $q(\mathbf{x}) \ll F^{r/2s}$. This raises the question whether the $1/2$ in the exponent of (1.8) is superfluous also in the cases $r = s+2$ or $s+1$ or s.

The case $r = s = 1$ is not covered by Theorem 3. It is an easy exercise to show that an indefinite binary quadratic form with integral coefficients has a zero $\mathbf{x} \in \mathbf{R}^2 \backslash \mathbf{0}$ with $q(\mathbf{x}) \ll F$, and that this is essentially best possible. So (1.8) is true also for $r = s = 1$, and in this case the $1/2$ in the exponent is necessary.

THEOREM 4. *Let $\mathfrak{F}$ be a quadratic form in $n \geq 5$ variables with coefficients in $\mathbf{Z}$. Let p be a prime. Then $\mathfrak{F}$ has a zero $\mathbf{x} \in \mathbf{Z}^n \backslash \mathbf{0}$ with $q_p(\mathbf{x}) \ll F^{c_n}$, where $c_n \leq cn^{-1/2}$ and the constant in $\ll$ depends only on n, p. More precisely, we may take $c_n = 4$, and when $n \geq 40$ and k is the largest integer with $8k(4k+1) \leq n$, we may take $c_n = 3/(2k)$.*

By Theorem 2 we must necessarily have $c_n \geq 2/(n-4)$. So the correct order of magnitude of c_n lies somewhere between n^{-1} and $n^{-1/2}$.

Now let $\mathfrak{F} \neq 0$ be a form with p-adic coefficients. Define $q_p(\mathfrak{F})$ as the maximum p-adic absolute value of the quotients of nonzero coefficients of $\mathfrak{F}$. Is it possible to assert that for $n \geq 5$ there is a zero $\mathbf{x} \in \mathbf{Q}_p^n \backslash \mathbf{0}$ with $q_p(\mathbf{x})$ bounded in terms

[2]Thus $\nu = \min(\mu_1, \nu^*)$, where ν^* is the third among $\lambda_1,\ldots,\lambda_r,\mu_1,\ldots,\mu_s$ when ordered according to size.

of $q_p(\mathfrak{F})$? The answer to this question is negative, as is seen from the following example. Let $p \neq 2$ and let u be a quadratic nonresidue modulo p. Set

$$\mathfrak{F} = (X_1 + \cdots + X_n)^2 - uX_1^2 - up^{2m}X_2^2 - \cdots - up^{2m(n-1)}X_n^2,$$

where m is large. Then $q_p(\mathfrak{F}) = 1$. Every zero is proportional to a "primitive" zero $\mathbf{x}$ which lies in $\mathbf{Z}_p^n$ but not in $p\mathbf{Z}_p^n$, where $\mathbf{Z}_p$ is the ring of p-adic integers. Let $\mathbf{x}$ be such a zero. Let l be such that $x_1 = \cdots = x_{l-1} = 0$ but $x_l \neq 0$; clearly $l \leq n-1$. We have $(x_1 + \cdots + x_n)^2 - up^{2m(l-1)}x_l^2 \equiv 0 \pmod{p^{2ml}}$, hence $p^m | x_l$, hence $q_p(\mathbf{x}) \geq p^m$. But m is arbitrarily large! (A similar example can be given with a real indefinite form.) The answer to the question is easily seen to be positive when $\mathfrak{F}$ is restricted to diagonal forms. The difficulty lies in the fact that $q_p(\mathbf{x})$ and $q_p(\mathfrak{F})$ are very sensitive to linear transformations.

However, we have the following.

THEOREM 5. *Let K be a field of characteristic $\neq 2$ with a nonarchimedean absolute value $|\cdots|$. Let $\mathfrak{F} = \sum_{i,j=1}^n f_{ij}X_iX_j$ be a form with coefficients $f_{ij} = f_{ji} \in K$ of absolute value ≤ 1. Write A_{ii} for the cofactor of f_{ii} in the coefficient matrix. Suppose that*

(a) $|f_{ii}| \geq B^{-1}$, *where* $B \geq 1$ $(1 \leq i \leq n)$,

(b) $|A_{ii}| \geq B^{-1}$ $(1 \leq i \leq n)$,

(c) $\mathfrak{F}$ *has a zero* $(w_1, \ldots, w_n) \in K^n$ *with each* $w_i \neq 0$.

Then $\mathfrak{F}$ has a zero $\mathbf{x} \in K^n$ with $q(\mathbf{x}) \ll B$, where q is defined in the obvious way, and the constant in $\ll$ depends only on K, $|\cdots|, n$.

In applications, when $\mathfrak{F}$ has a nontrivial zero, choose such a zero $\mathbf{w}$ with the least possible number of nonzero coordinates. Say $\mathbf{w} = (w_1, \ldots, w_l, 0, \ldots, 0)$ with $w_1 \cdots w_l \neq 0$. When $l = 1$, then $q(\mathbf{w}) = 1$. When $l > 1$, apply the theorem to $\hat{\mathfrak{F}}(X_1, \ldots, X_l) = \mathfrak{F}(X_1, \ldots, X_l, 0, \ldots, 0)$. The coefficients $\hat{f}_{ii}$ are not zero (otherwise $\hat{\mathfrak{F}}$ would have a zero $(0, \ldots, 1, \ldots, 0)$) and the cofactors $\hat{A}_{ii}$ are not zero (for if, say, $\hat{A}_{ll} = 0$, then $\hat{\mathfrak{F}}(X_1, \ldots, X_{l-1}, 0)$ is singular, hence has a nontrivial zero with $< l$ nonzero components). We thus get a zero $\mathbf{x}$ with

$$q(\mathbf{x}) \ll \max(|\hat{f}_{11}|^{-1}, \ldots, |\hat{f}_{ll}|^{-1}, |\hat{A}_{11}|^{-1}, \ldots, |\hat{A}_{ll}|^{-1}).$$

When $K = \mathbf{Q}$, $|\cdots|$ is the p-adic absolute value, and $\mathfrak{F}$ a form with coefficients in $\mathbf{Z}$ and with F as above, then $l \leq 5$ and $|\hat{f}_{ii}| \leq F$, $|\hat{A}_{ii}| \ll F^{l-1} \leq F^4$. We obtain a zero $\mathbf{x} \in \mathbf{Q}^n$ with $q_p(\mathbf{x}) \ll F^4$. This gives Theorem 4 with $c_n = 4$.

The details for the proof of Theorem 5 will be given only when $K = \mathbf{Q}$ or $\mathbf{Q}_p$ and when we deal with the p-adic absolute value.

2. Linear forms. Given a linear form $\mathfrak{L}$, write $|\mathfrak{L}|$ for the maximum modulus of its coefficients.

PROPOSITION 1. *Suppose $0 < l \leq s$. Given $D \geq 1$ there are linear forms*

$$\mathfrak{L}_i(\mathbf{Y}) = \mathfrak{L}(Y_1, \ldots, Y_s) \qquad (i = 1, \ldots, l)$$

with rational integer coefficients and with $|\mathfrak{L}_i| \leq D$ $(i = 1, \ldots, l)$ such that every nonzero complex vector $\mathbf{y} = (y_1, \ldots, y_s)$ has

$$\max(|\mathbf{y}|, |\mathfrak{L}_1(\mathbf{y})|, \ldots, |\mathfrak{L}_l(\mathbf{y})|) \gg D^{l/s}\langle \mathbf{y} \rangle. \tag{2.1}$$

The constant in $\gg$ here depends only on s.

This implies Theorem 1, as we now proceed to show. When C is small, we set $\mathfrak{F} = X_1^2 + \cdots + X_r^2 - X_{r+1}^2 - \cdots - X_{r+s}^2$, so that $F = 1$. Every nonzero $\mathbf{x}$ has $q(\mathbf{x}) \geq 1$, and this is $\gg C^{r/2s}$ when C is small. We may thus suppose that C is large. We put $D = [\rho C^{1/2}]$ with a constant $\rho = \rho(s)$ to be determined later. At any rate, $D \geq 1$ when C is large.

Write

$$r = sh + l \quad \text{with } 0 \leq l < s. \tag{2.2}$$

We will at first suppose that $l > 0$. We rename the variables $X_1, \ldots, X_n$ as Y_{ij} $(1 \leq i \leq s,\ 0 \leq j \leq h)$ and as $Y_1, \ldots, Y_l$; since $n = r+s = s(h+1)+l$, this makes sense. We further set

$$Z_{ij} = Y_{ij} - DY_{i,j-1} \qquad (1 \leq i \leq s,\ 1 \leq j \leq h), \tag{2.3}$$

$$Z_m = Y_m - \mathfrak{L}_m(Y_{1h}, \ldots, Y_{sh}) \qquad (1 \leq m \leq l), \tag{2.4}$$

where $\mathfrak{L}_1, \ldots, \mathfrak{L}_l$ are the forms of Proposition 1. We put

$$\mathfrak{F} = \sum_{i=1}^{s} \sum_{j=1}^{h} Z_{ij}^2 + \sum_{m=1}^{l} Z_m^2 - \sum_{i=1}^{s} Y_{i0}^2.$$

Then $\mathfrak{F}$ has integer coefficients and is of the type (r, s). Moreover, $F \ll D^2$, so that $F \leq C$ if ρ was chosen sufficiently small.

Now let $\mathbf{x} \neq \mathbf{0}$ be real with $\mathfrak{F}(\mathbf{x}) \leq 0$. Define y_{ij}, y_m $(1 \leq i \leq s,\ 0 \leq j \leq h,\ 1 \leq m \leq l)$, as well as z_{ij}, z_m, in the obvious way. Set $\mathbf{y} = (y_{10}, \ldots, y_{s0})$. By our construction of $\mathfrak{F}$, and since $\mathfrak{F}(\mathbf{x}) \leq 0$, we have $\mathbf{y} \neq \mathbf{0}$. Again, since $\mathfrak{F}(\mathbf{x}) \leq 0$, we have

$$|z_{ij}| \ll |\mathbf{y}|, \qquad |z_m| \ll |\mathbf{y}|.$$

Thus

$$y_{ij} = Dy_{i,j-1} + z_{ij} = Dy_{i,j-1} + O(|\mathbf{y}|) \qquad (1 \leq i \leq s,\ 1 \leq j \leq h).$$

We have $y_{i1} = Dy_{i0} + O(|\mathbf{y}|)$, $y_{i2} = Dy_{i1} + O(|\mathbf{y}|) = D^2 y_{i0} + O(D|\mathbf{y}|)$, etc., and finally

$$y_{ih} = D^h y_{i0} + O(D^{h-1}|\mathbf{y}|) \qquad (1 \leq i \leq s). \tag{2.5}$$

We further have

$$y_m = \mathfrak{L}_m(y_{1h}, \ldots, y_{sh}) + z_m = \mathfrak{L}_m(y_{1h}, \ldots, y_{sh}) + O(|\mathbf{y}|) = D^h \mathfrak{L}_m(\mathbf{y}) + O(D^h|\mathbf{y}|)$$

since $|\mathfrak{L}_m| \leq D$, and therefore

$$y_m = D^h(\mathfrak{L}_m(\mathbf{y}) + O(|\mathbf{y}|)) \qquad (1 \leq m \leq l). \tag{2.6}$$

We now distinguish two cases.

Either $|\mathbf{y}|$ is small as compared to $D^{l/s}\langle \mathbf{y} \rangle$, say $|\mathbf{y}| \leq \delta(s) D^{l/s}\langle \mathbf{y} \rangle$. Then if $\delta(s)$ is small enough, (2.1) shows that there is an m in $1 \leq m \leq l$ with $|\mathfrak{L}_m(\mathbf{y})| \gg D^{l/s}\langle \mathbf{y} \rangle$. Hence, again when $\delta(s)$ is small, (2.6) yields

$$|y_m| \gg D^{h+(l/s)}\langle \mathbf{y} \rangle = D^{r/s}\langle \mathbf{y} \rangle.$$

Since y_m and the components of $\mathbf{y}$ are among the components of $\mathbf{x}$, we obtain $q(\mathbf{x}) \gg D^{r/s} \gg C^{r/2s}$, as desired.

Or we have $|\mathbf{y}| > \delta(s)D^{l/s}\langle\mathbf{y}\rangle$. Say $|y_{i0}| = |\mathbf{y}| \gg D^{l/s}\langle\mathbf{y}\rangle$ for some particular i in $1 \le i \le s$. Then (2.5) gives

$$|y_{ih}| \gg D^{h+(l/s)}\langle\mathbf{y}\rangle = D^{r/s}\langle\mathbf{y}\rangle,$$

and again $q(\mathbf{x}) \gg C^{r/2s}$.

This completes the proof when $l > 0$. The case $l = 0$ is simpler, and the Y_m, Z_m and forms $\mathfrak{L}_m$ $(1 \le m \le l)$ disappear from the argument. We may omit the details, all the more so, since this case follows from Watson's result quoted above.

3. Proof of Proposition 1. We proceed by induction on l. We may suppose that D is large. When $l = 1$, set $E = [D^{1/s}]$ and

$$\mathfrak{L}_1(\mathbf{Y}) = EY_1 + E^2Y_2 + \cdots + E^sY_s.$$

Then $|\mathfrak{L}_1| \le E^s \le D$. Suppose $y = (y_1, \dots, y_s)$ has $y_k \ne 0$ but $y_j = 0$ for $k < j \le s$. Either $|y_i| \le (2s)^{-1}E|y_k|$ for $1 \le i < k$. Then $|\mathfrak{L}_1(\mathbf{y})| \ge \frac{1}{2}E^k|y_k| \gg D^{1/s}\langle\mathbf{y}\rangle$, and we are done. Or some $|y_i| > (2s)^{-1}E|y_k| \gg D^{1/s}|y_k| \ge D^{1/s}\langle\mathbf{y}\rangle$, and again we are done.

Suppose now that the proposition is true for $1, 2, \dots, l-1$ where $l \ge 2$. Write

$$s = ml + v \quad \text{with } 0 \le v < l. \tag{3.1}$$

Now when $v = 0$, divide the s variables into $\mathbf{Y}_1 = (Y_{11}, \dots, Y_{1m}), \dots, \mathbf{Y}_l = (Y_{l1}, \dots, Y_{lm})$. By the case $l = 1$, there is a form $\mathfrak{L}(Z_1, \dots, Z_m) = \mathfrak{L}(\mathbf{Z})$ in m variables such that $|\mathfrak{L}| \le D$ and

$$\max(|\mathbf{z}|,\ |\mathfrak{L}(\mathbf{z})|) \gg D^{1/m}\langle\mathbf{z}\rangle$$

for each $\mathbf{z}$. Set $\mathfrak{L}_i(\mathbf{Y}) = \mathfrak{L}(\mathbf{Y}_i)$ $(i = 1, \dots, l)$. Then if, say, $\mathbf{y}_i = (y_{i1}, \dots, y_{im}) \ne \mathbf{0}$, we have

$$\max(|\mathbf{y}|, |\mathfrak{L}_1(\mathbf{y})|, \dots, |\mathfrak{L}_l(\mathbf{y})|) \ge \max(|\mathbf{y}_i|, |\mathfrak{L}(\mathbf{y}_i)|) \gg D^{1/m}\langle\mathbf{y}_i\rangle \ge D^{l/s}\langle\mathbf{y}\rangle.$$

We may therefore suppose that $v > 0$, and we write

$$l = uv + w \quad \text{with } 0 \le w < v. \tag{3.2}$$

We now relabel the variables $Y_1, \dots, Y_s$ as follows.

(i) Variables Y_j with $1 \le j \le v$,

(ii) Variables Y_{ijk} with $1 \le i \le u,\ 1 \le j \le v,\ 1 \le k \le m$.

When $w > 0$, we have further

(iii) Variables Y_{tk} with $1 \le t \le w,\ 1 \le k \le m$.

Since $s = v + uvm + wm$, this always gives the correct number of variables. We set

$$\mathbf{Y}_{ij} = (Y_{ij1}, \dots, Y_{ijm}) \qquad (1 \le i \le u,\ 1 \le j \le v),$$

and when $w > 0$, we further set

$$\mathbf{Y}_t = (Y_{t1}, \dots, Y_{tm}) \qquad (1 \le t \le w).$$

We put $E = [\varepsilon D^{1/s}]$ with $\varepsilon = \varepsilon(s) > 0$ to be chosen later. We introduce the linear forms

$$\mathfrak{M}_{0j} = E^{ml}Y_j \qquad (1 \le j \le v),$$

$$\mathfrak{M}_{ij} = \mathfrak{M}_{ij}(\mathbf{Y}_{ij}) = E^l Y_{ij1} + E^{2l} Y_{ij2} + \cdots + E^{ml} Y_{ijm} \qquad (1 \le i \le u,\ 1 \le j \le v).$$

Then $|\mathfrak{M}_{ij}| \le E^{ml}$ $(0 \le i \le u,\ 1 \le j \le v)$. Further set

$$\mathfrak{L}_{ij} = \mathfrak{M}_{ij} - E^v \mathfrak{M}_{i-1,j} \qquad (1 \le i \le u,\ 1 \le j \le v).$$

In the case when $w > 0$ we are not yet finished: Put

$$\mathfrak{M}_t = \mathfrak{M}_t(\mathbf{Y}_t) = E^l Y_{t1} + E^{2l} Y_{t2} + \cdots + E^{ml} Y_{tl} \qquad (1 \le t \le w),$$

so that also $|\mathfrak{M}_t| \le E^{ml}$. Further let $\mathfrak{N}_t(Z_1, \ldots, Z_v)$ $(1 \le t \le w)$ be the forms of the proposition, with w, v, E^v in place of l, s, D, respectively.[3] Thus $|\mathfrak{N}_t| \le E^v$, and for $\mathbf{z} = (z_1, \ldots, z_v) \ne \mathbf{0}$ we have

$$\max(|\mathbf{z}|, |\mathfrak{N}_1(\mathbf{z})|, \ldots, |\mathfrak{N}_w(\mathbf{z})|) \gg E^{v(w/v)} \langle \mathbf{z} \rangle = E^w \langle \mathbf{z} \rangle. \tag{3.3}$$

Finally put

$$\mathfrak{L}_t = \mathfrak{M}_t - \mathfrak{N}_t(\mathfrak{M}_{u1}, \ldots, \mathfrak{M}_{uv}) \qquad (1 \le t \le w).$$

The forms $\mathfrak{L}_{ij}$ in the case when $w = 0$, and the forms $\mathfrak{L}_{ij}$ together with the forms $\mathfrak{L}_t$ when $w > 0$, are altogether $uv + w = l$ forms, and we claim that these l forms have the properties enunciated in the proposition. Clearly it does not matter that they are not simply numbered as $\mathfrak{L}_1, \ldots, \mathfrak{L}_l$. First, it is obvious that $|\mathfrak{L}_{ij}|, |\mathfrak{L}_t|$ are $\ll E^{ml+v} = E^s$, so that when $\varepsilon > 0$ above was chosen sufficiently small, they are $\le D$, as required. It remains for us to show that for $\mathbf{y} = (y_1, \ldots, y_s) \ne \mathbf{0}$ we have (2.1), i.e.,

$$\max(|\mathbf{y}|, |\mathfrak{L}_{11}(\mathbf{y})|, \ldots, |\mathfrak{L}_{uv}(\mathbf{y})|, |\mathfrak{L}_1(\mathbf{y})|, \ldots, |\mathfrak{L}_w(\mathbf{y})|) \gg E^l \langle \mathbf{y} \rangle. \tag{3.4}$$

Suppose then that $\mathbf{y} \ne \mathbf{0}$. Denote its components by y_j $(1 \le j \le v)$, by y_{ijk} $(1 \le i \le u,\ 1 \le j \le v,\ 1 \le k \le m)$, and further by y_{tk} $(1 \le t \le w,\ 1 \le k \le m)$ when $w > 0$, and introduce vectors $\mathbf{y}_{ij}$ and $\mathbf{y}_t$. Let $\mathfrak{S}$ be the subset of $\{1, \ldots, v\}$ consisting of the indices j with $y_j \ne 0$.

We now make the following observation, which is proved like the case $l = 1$ of the proposition: When $\mathbf{y}_{ij} \ne \mathbf{0}$, then

$$\max(|\mathbf{y}_{ij}|, |\mathfrak{M}_{ij}(\mathbf{y}_{ij})|) \gg E^l \langle \mathbf{y}_{ij} \rangle \qquad (1 \le i \le u,\ 1 \le j \le v). \tag{3.5}$$

Similarly, when $w > 0$, then each $\mathbf{y}_t \ne \mathbf{0}$ has

$$\max(|\mathbf{y}_t|, |\mathfrak{M}_t(\mathbf{y}_t)|) \gg E^l \langle \mathbf{y}_t \rangle \qquad (1 \le t \le w). \tag{3.6}$$

Suppose now that $j \notin \mathfrak{S}$ is fixed for the moment. We have $y_j = 0$, hence $\mathfrak{M}_{0j}(\mathbf{y}) = 0$, hence $\mathfrak{L}_{1j}(\mathbf{y}) = \mathfrak{M}_{1j}(\mathbf{y}_{1j})$. It follows from (3.5) that when $\mathbf{y}_{1j} \ne \mathbf{0}$, then either $|\mathbf{y}| \gg E^l \langle \mathbf{y} \rangle$ or $|\mathfrak{L}_{1j}(\mathbf{y})| \gg E^l \langle \mathbf{y} \rangle$, and in both cases (3.4) is true. We may therefore suppose that $\mathbf{y}_{1j} = \mathbf{0}$. Then $\mathfrak{L}_{2j}(\mathbf{y}) = \mathfrak{M}_{2j}(\mathbf{y}_{2j})$. Reasoning as before, we see that we may suppose that $\mathbf{y}_{2j} = \mathbf{0}$, etc. Hence we may suppose that

$$\mathbf{y}_{1j} = \mathbf{y}_{2j} = \cdots = \mathbf{y}_{uj} = \mathbf{0} \quad \text{for each } j \notin \mathfrak{S}, \tag{3.7}$$

so that in particular

$$\mathfrak{M}_{uj}(\mathbf{y}) = 0 \quad \text{for each } j \notin \mathfrak{S}. \tag{3.8}$$

[3] By (3.1), (3.2) our induction involves the complete quotients in the continued fraction expansion of s/l, more precisely every second quotient.

Next, suppose that $j \in \mathfrak{S}$ is fixed at the moment. We have $E^v\mathfrak{M}_{0j}(\mathbf{y}) = E^{ml+v}y_j = E^s y_j$. Thus if $|\mathfrak{M}_{1j}(\mathbf{y})|$ is small in comparison to $E^s|y_j|$, then $|\mathfrak{L}_{1j}(\mathbf{y})| \gg E^s|y_j| \geq E^s\langle\mathbf{y}\rangle$, and (3.4) holds. We may thus suppose that $|\mathfrak{M}_{1j}(\mathbf{y})| \gg E^s|y_j|$, which yields $E^v|\mathfrak{M}_{1j}(\mathbf{y})| \gg E^{s+v}|y_j|$. If $|\mathfrak{M}_{2j}(\mathbf{y})|$ is small in comparison to $E^{s+v}|y_j|$, then $|\mathfrak{L}_{2j}(\mathbf{y})| \gg E^{s+v}|y_j| \geq E^{s+v}\langle\mathbf{y}\rangle$, and again (3.4) holds. We may thus suppose that $|\mathfrak{M}_{2j}(\mathbf{y})| \gg E^{s+v}|y_j|$. Continuing in this manner we see eventually that we may suppose that

$$|\mathfrak{M}_{uj}(\mathbf{y})| \gg E^{s+(u-1)v}|y_j| \quad \text{for each } j \in \mathfrak{S}. \tag{3.9}$$

In the case when $w = 0$, the set $\mathfrak{S}$ cannot be empty by (3.7) and since $\mathbf{y} \neq \mathbf{0}$. For $j \in \mathfrak{S}$ we have

$$|\mathfrak{M}_{uj}(\mathbf{y})| \gg E^{ml+v+(u-1)v}|y_j| = E^{ml+l}|y_j|$$

by (3.9), (3.1), (3.2). Since $|\mathfrak{M}_{uj}(\mathbf{y})| \ll E^{ml}|\mathbf{y}_{uj}|$, we obtain $|\mathbf{y}_{uj}| \gg E^l|y_j|$, whence (3.4).

It remains for us to deal with the case when $w > 0$. Introduce

$$\mathbf{z} = (\mathfrak{M}_{u1}(\mathbf{y}), \dots, \mathfrak{M}_{uv}(\mathbf{y})).$$

Now if $\mathfrak{S} = \emptyset$, then some $\mathbf{y}_t \neq \mathbf{0}$ by (3.7) and since $\mathbf{y} \neq \mathbf{0}$. Further $\mathbf{z} = \mathbf{0}$ by (3.8), so that $\mathfrak{L}_t(\mathbf{y}) = \mathfrak{M}_t(\mathbf{y}_t)$. By (3.6) we have either $|\mathbf{y}_t| \gg E^l\langle\mathbf{y}_t\rangle$ or $|\mathfrak{L}_t(\mathbf{y})| \gg E^l\langle\mathbf{y}_t\rangle$, and in both cases (3.4) holds.

We may thus suppose that $\mathfrak{S} \neq \emptyset$; then $\mathbf{z} \neq \mathbf{0}$ by (3.9). In view of (3.3) we either have $|\mathbf{z}| \gg E^w\langle\mathbf{z}\rangle$, or some $|\mathfrak{N}_t(\mathbf{z})| \gg E^w\langle\mathbf{z}\rangle$. In the first subcase there are i, j in $\mathfrak{S}$ with $|\mathfrak{M}_{ui}(\mathbf{y})| \gg E^w|\mathfrak{M}_{uj}(\mathbf{y})|$. In conjunction with (3.9), (3.1), (3.2) this yields

$$|\mathfrak{M}_{ui}(\mathbf{y})| \gg E^{w+ml+v+uv-v}|y_j| = E^{ml+l}|y_j| \geq E^{ml+l}\langle\mathbf{y}\rangle.$$

Since $|\mathfrak{M}_{ui}(\mathbf{y})| \ll E^{ml}|\mathbf{y}_{ui}|$, we obtain $|\mathbf{y}_{ui}| \gg E^l\langle\mathbf{y}\rangle$, and (3.4). In the second subcase, by (3.9),

$$|\mathfrak{N}_t(\mathbf{z})| \gg E^w\langle\mathbf{z}\rangle \gg E^{w+ml+v+uv-v}\langle\mathbf{y}\rangle = E^{ml+l}\langle\mathbf{y}\rangle.$$

Then either $|\mathfrak{L}_t(\mathbf{y})| \gg E^l\langle\mathbf{y}\rangle$ and we are done, or $|\mathfrak{M}_t(\mathbf{y})| \gg E^{ml+l}\langle\mathbf{y}\rangle$. Since $|\mathfrak{M}_t(\mathbf{y})| \ll E^{ml}|\mathbf{y}_t|$, we may infer that $|\mathbf{y}_t| \gg E^l\langle\mathbf{y}\rangle$, hence (3.4).

4. The p-adic case. Just as in the real case we begin with a proposition on linear forms.

PROPOSITION 2. *Suppose $0 < l \leq s$. Given $D \geq 1$ there are linear forms $\mathfrak{L}_i(\mathbf{Y}) = \mathfrak{L}_i(Y_1, \dots, Y_s)$ $(i = 1, \dots, l)$ whose coefficients are rational with (standard) absolute value ≤ 1 and with denominators which are powers of p and not larger than D, such that every nonzero $\mathbf{y} \in \mathbf{Q}_p^s$ has*

$$\max(|\mathbf{y}|_p,\ |\mathfrak{L}_1(\mathbf{y})|_p, \dots, |\mathfrak{L}_l(\mathbf{y})|_p) \gg D^{l/s}\langle\mathbf{y}\rangle.$$

The constant in $\gg$ here depends only on s and on p.

The proof of this proposition is like that of Proposition 1. Let δ be the largest integer with $p^{\delta s} \leq D$, and set $E = p^{-\delta}$. The construction of the forms is essentially the same as in §3. In some cases E is to be replaced by $|E|_p = p^{\delta}$. For instance, when $l = 1$, we set again $\mathfrak{L}_1(\mathbf{Y}) = EY_1 + \cdots + E^sY_s$. The denominators are $\leq |E|_p^s \leq D$. Or, when $l > 1$ and when $w > 0$, the forms $\mathfrak{N}_t(Z_1, \dots, Z_v)$ $(t = 1, \dots, w)$ are

the forms of Proposition 2 with $w, v, |E|_p^v$ in place of l, s, D. When D and hence δ is large, the forms $\mathfrak{L}_{ij}, \mathfrak{L}_t$ will have coefficients of absolute value < 1. The denominators of these coefficients will be powers of p, and will be $\leq |E|_p^{ml+v} = |E|_p^s = p^{\delta s} \leq D$.

Before embarking on the deduction of Theorem 2, we insert

LEMMA 1. *Set*

$$\mathfrak{G}(\mathbf{Z}) = \mathfrak{G}(Z_1, Z_2, Z_3, Z_4) = Z_1^2 - uZ_2^2 + p(Z_3^2 - uZ_4^2),$$

where u is a quadratic nonresidue modulo p when p is odd, and $u = -1$ when $p = 2$. Then for each $\mathbf{z} \in \mathbf{Q}_p^4 \backslash \mathbf{0}$ we have $|\mathfrak{G}(\mathbf{z})|_p \geq p^{-3}|\mathbf{z}|_p^2$.

PROOF. When $p \neq 2$, then

$$|z_1^2 - uz_2^2|_p = \max(|z_1|_p^2, |z_2|_p^2)$$

and

$$|p(z_3^2 - uz_4^2)|_p = p^{-1} \max(|z_3|_p^2, |z_4|_p^2),$$

and since these cannot be equal,

$$|\mathfrak{G}(\mathbf{z})|_p = \max(|z_1|_p^2, |z_2|_p^2, p^{-1}|z_3|_p^2, p^{-1}|z_4|_p^2) \geq p^{-1}|\mathbf{z}|_p^2.$$

When $p = 2$, we may suppose by homogeneity that $|\mathbf{z}|_p = 1$, so that in particular the z_i are p-adic integers. When $\max(|z_1|_p, |z_2|_p) = 1$, then $\mathfrak{G}(\mathbf{z}) \not\equiv 0 \pmod 8$, so that $|\mathfrak{G}(\mathbf{z})|_p \geq 2^{-2} = 2^{-2}|\mathbf{z}|_p^2$. When $\max(|z_1|_p, |z_2|_p) < 1$ and $\max(|z_3|_p, |z_4|_p) = 1$, then $\mathfrak{G}(\mathbf{z})$ is even but $\not\equiv 0 \pmod{16}$, so that $|\mathfrak{G}(\mathbf{z})|_p \geq 2^{-3} = 2^{-3}|\mathbf{z}|_p^2$.

Now, in order to prove Theorem 2, it clearly will suffice to construct a quadratic form $\mathfrak{F}_1$ whose coefficients are not necessarily integers but are rational numbers of (standard) absolute value ≤ 1, and with denominators which are powers of p and not larger than C. For then $\mathfrak{F} = p^\beta \mathfrak{F}_1$, where p^β is the least common denominator of the coefficients of $\mathfrak{F}_1$, will have the desired properties. We may suppose C to be large and we set $D = p^{-\delta}$, where δ is the largest integer with $p^{2\delta+\gamma} \leq C$, with a constant $\gamma = \gamma(n, p) > 0$ to be determined later.

The construction for Theorem 2 is analogous to that for Theorem 1, with r, s replaced by $4, n-4$ respectively. Thus (2.2) becomes

$$4 = (n-4)h + l \quad \text{with } 0 \leq l < n-4,$$

and $X_1, \ldots, X_n$ are renamed as Y_{ij} $(1 \leq i \leq n-4,\ 0 \leq j \leq h)$ and $Y_1, \ldots, Y_l$. Linear forms Z_{ij} and Z_m are defined as in (2.3), (2.4), where $\mathfrak{L}_1, \ldots, \mathfrak{L}_l$ are the forms of Proposition 2, with $|D|_p = p^\delta$ in place of D. Thus for example, when $n = 5$, then $h = 4$, $l = 0$, the variables $X_1, \ldots, X_5$ become $Y_{10}, \ldots, Y_{14}$, and the Z's are given by

$$Z_{1j} = Y_{1j} - DY_{1,j-1} \qquad (1 \leq j \leq 4).$$

On the other hand when $n \geq 9$, then $h = 0$, $l = 4$, and the variables become $Y_{10}, \ldots, Y_{n-4,0}$ and $Y_1, \ldots, Y_4$, and the Z's are

$$Z_m = Y_m - \mathfrak{L}_m(Y_{10}, \ldots, Y_{n-4,0}) \qquad (1 \leq m \leq 4).$$

In every case there are four linear forms Z, they form a 4-tuple $\mathbf{Z}$, and $\mathfrak{G}(\mathbf{Z})$ is well defined. We put

$$\mathfrak{F}_0 = \mathfrak{G}(\mathbf{Z}) + \sum_{i=1}^{n-4} Y_{i0}^2. \tag{4.1}$$

The coefficients of $\mathfrak{F}_0$ are $\ll 1$, and $\mathfrak{F}_1 = p^{-\gamma}\mathfrak{F}_0$ with suitable $\gamma = \gamma(n,p) > 0$ has coefficients of (standard) absolute value ≤ 1. The coefficients of $\mathfrak{F}_1$ have denominators which are powers of p and which do not exceed $p^{2\delta+\gamma} \le C$.

Now let $\mathbf{x} \neq \mathbf{0}$ be a p-adic zero of $\mathfrak{F}_1$. Define y_{ij}, y_m, z_{ij}, z_m in the obvious way, put $\mathbf{y} = (y_{10}, \dots, y_{n-4,0})$ and combine the four z's into $\mathbf{z}$. In view of $\mathfrak{F}_0(\mathbf{x}) = 0$ and the lemma we obtain $|\mathbf{z}|_p \ll |\mathbf{y}|_p$. Thus

$$|y_{ij}|_p = |Dy_{i,j-1}|_p + O(|\mathbf{y}|_p) \qquad (1 \le i \le n-4,\ 1 \le j \le h),$$

whence

$$|y_{ih}|_p = |D^h y_{i0}|_p + O(|D^{h-1}\mathbf{y}|_p) \qquad (1 \le i \le n-4),$$

which is the analogue of (2.5). Further

$$|y_m|_p = |D|_p^h(|\mathfrak{L}_m(\mathbf{y})|_p + O(|\mathbf{y}|_p) \qquad (1 \le m \le l),$$

which corresponds to (2.6). The rest of the argument is very close to that in §2.

By choosing appropriate signs in $\mathfrak{G}$ and in front of the terms Y_{i0}^2 in (4.1) we can modify the construction so as to obtain a form $\mathfrak{F}_0$, hence $\mathfrak{F}$, of prescribed type (r,s).

5. Proof of Theorem 3. Let $\mathfrak{L}_1(\mathbf{X}), \dots, \mathfrak{L}_k(\mathbf{X})$ be linear forms with $|\mathfrak{L}_i| = 1$ $(i = 1, \dots, k)$. Generalizing (1.7) we will show that $\mathfrak{F}$ has a real zero $\mathbf{x} \neq \mathbf{0}$ with

$$|\mathfrak{L}_i(\mathbf{x})| \gg (\nu/\lambda_1)^{1/2}|\mathbf{x}| \qquad (i = 1, \dots, k), \tag{5.1}$$

with a constant in $\gg$ depending only on n and k. After an orthogonal linear transformation ($|\mathbf{x}|$ and $|\mathfrak{L}_i|$ change only by bounded factors under such a transformation), we may suppose that

$$\mathfrak{F} = \lambda_1 X_1^2 + \cdots + \lambda_r X_r^2 - \mu_1 X_{r+1}^2 - \cdots - \mu_s X_{r+s}^2. \tag{5.2}$$

We begin with the case when

$$r \ge 2 \quad \text{and} \quad \lambda_2 \ge \mu_1, \tag{5.3}$$

so that $\nu = \mu_1$. Let t be the largest number in $2 \le t \le r$ with $\lambda_t \ge \nu/8n$. Let Π be the set of points $\mathbf{y} = (y_1, \dots, y_n)$ with $(y_1, \dots, y_t)$ on the unit sphere $y_1^2 + \cdots + y_t^2 = 1$ and with $(y_{t+1}, \dots, y_n)$ in the cube $1 \le y_i \le 2$ $(i = t+1, \dots, n)$. We shall need the measure μ on Π which is the product of the spherical measure, normalized so that the total measure is 1, and the Euclidean measure on the cube. The form

$$g(\mathbf{Y}) = -\lambda_{t+1}Y_{t+1}^2 - \cdots - \lambda_r Y_r^2 + \mu_1 Y_{r+1}^2 + \cdots + \mu_s Y_{r+s}^2$$

has

$$\tfrac{1}{2}\nu = \mu_1 - 4n(\mu_1/8n) \le g(\mathbf{y}) \le 4n\nu \tag{5.4}$$

for $\mathbf{y} \in \Pi$. The map

$$\sigma(\mathbf{y}) = (y_1(g(\mathbf{y})/\lambda_1)^{1/2}, \dots, y_t(g(\mathbf{y})/\lambda_t)^{1/2}, y_{t+1}, \dots, y_n)$$

maps Π into the zero set of $\mathfrak{F}$. Moreover, $1 \ll |\sigma(\mathbf{y})| \ll 1$ for $\mathbf{y} \in \Pi$. Thus to prove the assertion on (5.1) it will be enough to show that there is a $\mathbf{y} \in \Pi$ with

$$|\mathfrak{L}_i(\sigma(\mathbf{y}))| \gg (\nu/\lambda_1)^{1/2} \qquad (i = 1, \dots, k).$$

We will do this by proving that for any linear form $\mathfrak{L}$ with $|\mathfrak{L}| = 1$ the elements $\mathbf{y} \in \Pi$ with

$$|\mathfrak{L}(\sigma(\mathbf{y}))| \leq \varepsilon(\nu/\lambda_1)^{1/2} \tag{5.5}$$

have a μ-measure which tends to zero as $\varepsilon \to 0$, independent of $\mathfrak{L}$ and $\mathfrak{F}$.

Given $\mathfrak{L} = c_1X_1 + \cdots + c_nX_n$ put $\hat{c} = \max(|c_{t+1}|, \ldots, |c_n|)$. Suppose that $0 < \varepsilon < 1$. We distinguish two subcases.

Case A.

$$|c_i|(\nu/\lambda_i)^{1/2} \leq \varepsilon^{1/2}\hat{c} \qquad (i = 1, \ldots, t). \tag{5.6}$$

We claim that

$$\varepsilon^{1/2}\hat{c} > \varepsilon(\nu/\lambda_1)^{1/2}. \tag{5.7}$$

This is obvious when $\hat{c} = 1$. When $\hat{c} < 1$, there is a j in $1 \leq j \leq t$ having $|c_j| = 1$, so that (5.6) yields $\varepsilon^{1/2}\hat{c} \geq (\nu/\lambda_j)^{1/2} \geq (\nu/\lambda_1)^{1/2} > \varepsilon(\nu/\lambda_1)^{1/2}$.

The points $\mathbf{y} \in \Pi$ with

$$|c_{t+1}y_{t+1} + \cdots + c_ny_n| \leq 3n^2\hat{c}\varepsilon^{1/2}$$

form a set of μ-measure $\ll \varepsilon^{1/2}$. For points $\mathbf{y} \in \Pi$ outside this set we have

$$|\mathfrak{L}(\sigma(\mathbf{y}))| > 3n^2\hat{c}\varepsilon^{1/2} - \sum_{i=1}^{t} |c_i| \left(\frac{4n\nu}{\lambda_i}\right)^{1/2} > \varepsilon^{1/2}\hat{c} > \varepsilon(\nu/\lambda_1)^{1/2}$$

by (5.4), (5.6), (5.7).

Case B. There is an i in $1 \leq i \leq t$ with

$$|c_i|(\nu/\lambda_i)^{1/2} > \varepsilon^{1/2}\hat{c}. \tag{5.8}$$

Put $\mathbf{Y}_0 = (Y_1, \ldots, Y_t)$ and $\mathfrak{M}(\mathbf{Y}_0) = c_1(\nu/\lambda_1)^{1/2}Y_1 + \cdots + c_t(\nu/\lambda_t)^{1/2}Y_t$. Either $\hat{c} = 1$, and then $|\mathfrak{M}| \gg \varepsilon^{1/2}$ by (5.8). Or some $|c_j| = 1$ where $1 \leq j \leq t$, and then $|\mathfrak{M}| \gg (\nu/\lambda_j)^{1/2} \geq (\nu/\lambda_1)^{1/2}$. So always

$$|\mathfrak{M}| \gg \min(\varepsilon^{1/2}, (\nu/\lambda_1)^{1/2}). \tag{5.9}$$

When $y_{t+1}, \ldots, y_n$ are fixed, then

$$\mathfrak{L}(\sigma(\mathbf{y})) = a\mathfrak{M}(\mathbf{y}_0) + b,$$

where $a = (g(\mathbf{y})/\nu)^{1/2}$ and b are fixed. Since $|a| \geq 2^{-1/2}$ by (5.4), the relation (5.5) implies

$$|\mathfrak{M}(\mathbf{y}_0) + c| \leq 2^{1/2}\varepsilon(\nu/\lambda_1)^{1/2} \tag{5.10}$$

with $c = b/a$. This defines a strip in t-dimensional space of width

$$\ll \varepsilon(\nu/\lambda_1)^{1/2}|\mathfrak{M}|^{-1} \ll \max(\varepsilon^{1/2}(\nu/\lambda_1)^{1/2}, \varepsilon) \leq \varepsilon^{1/2}.$$

The intersection of this strip with the sphere $y_1^2 + \cdots + y_t^2 = 1$ has a spherical measure which tends to zero as $\varepsilon \to 0$.

This finishes the proof in the case (5.3), i.e. in the first case of (1.5). Suppose now that we are in the second or third case of (1.5). Thus $\lambda_1 \geq \mu_1 > \lambda_2$. After renumbering of the variables, the diagonal form (5.2) becomes

$$\mathfrak{F} = \lambda_1X_1^2 - \mu_1X_2^2 \pm \nu X_3^2 + \rho_4X_4^2 + \cdots + \rho_nX_n^2$$

with $|\rho_i| \le \nu$ $(4 \le i \le n)$. In the second case of (1.5) we have the + sign and $\nu = \lambda_2$, while in the third case we have the − sign and $\nu = \mu_2$.

Our proof will be similar to the case (5.3) already done, with $t = 2$ and $\mathbf{Y}_0 = (Y_1, Y_2)$. Let H be the set of points (y_1, y_2) with $|y_2| \le 1$ on the hyperbola $y_1^2 - y_2^2 = 1$. Let μ_0 be the length-measure on H, normalized such that $\mu_0(H) = 1$. This time Π will consist of $(y_1, \dots, y_n)$ with $(y_1, y_2) \in H$ and with $(y_3, \dots, y_n)$ in the cube $n \le y_3 \le n+1$, $0 \le y_4, \dots, y_n \le 1$. Further, μ will be the product of μ_0 and the Euclidean measure on the cube. The quadratic form

$$g(\mathbf{Y}) = \mp\nu Y_3^2 - \rho_4 Y_4^2 - \cdots - \rho_n Y_n^2$$

has

$$(n^2 - 2n)\nu \le \mp g(\mathbf{y}) \le (n+2)^2\nu \tag{5.11}$$

for $\mathbf{y} \in \Pi$. The map

$$\sigma(\mathbf{y}) = (y_1(\pm g(\mathbf{y})/\lambda_1)^{1/2}, y_2(\pm g(\mathbf{y})/\mu_1)^{1/2}, y_3, \dots, y_n)$$

maps Π into the zero set of $\mathfrak{F}$. Moreover, (5.11) yields $1 \ll |\sigma(\mathbf{y})| \ll 1$ for $\mathbf{y} \in \Pi$.

Given $\mathfrak{L}$ with $|\mathfrak{L}| = 1$, we will again show that the $\mathbf{y} \in \Pi$ with (5.5) have a μ-measure which tends to zero as $\varepsilon \to 0$. We put $\hat{c} = \max(|c_3|, \dots, |c_n|)$, and the subcases are

Case A. $\max(|c_1|(\nu/\lambda_1)^{1/2}, |c_2|(\nu/\mu_1)^{1/2}) < \varepsilon^{1/2}\hat{c}$.

Case B. When this maximum is $> \varepsilon^{1/2}\hat{c}$.

The argument in either case is very much like before. In Case B we set $\mathfrak{M}(\mathbf{Y}_0) = c_1(\nu/\lambda_1)^{1/2}Y_1 + c_2(\nu/\mu_1)^{1/2}Y_2$. Again (5.9) holds. When $y_3, \dots, y_n$ are fixed, then $\mathfrak{L}(\sigma(\mathbf{y})) = a\mathfrak{M}(\mathbf{y}_0) + b$, where $a = (\pm g(y)/\nu)^{1/2}$ and b are fixed. Since $|a| > 1 > 2^{-1/2}$ by (5.11), the relation (5.5) again implies (5.10). Thus $\mathbf{y}_0$ lies in a strip in the plane of width $\ll \varepsilon^{1/2}$. The intersection of this strip with H has a μ_0-measure which tends to zero as $\varepsilon \to 0$.

6. Representation of diagonal forms. Let us recall the well-known Siegel Lemma.

Let $\mathfrak{L}_1(\mathbf{X}), \dots, \mathfrak{L}_k(\mathbf{X})$ be linear forms with rational integer coefficients in $l > k$ variables. These forms have a common zero $\mathbf{x} \in \mathbf{Z}^l \backslash \mathbf{0}$ with

$$|\mathbf{x}| \ll (|\mathfrak{L}_1| \cdots |\mathfrak{L}_k|)^{1/(l-k)}.$$

A quadratic form $\mathfrak{G}(X_1, \dots, X_m)$ is *diagonal* if it is of the form $a_1X_1^2 + \cdots + a_mX_m^2$. This happens precisely when

$$\mathfrak{G}(\mathbf{e}_i, \mathbf{e}_j) = 0 \qquad (1 \le i < j \le m),$$

where $\mathfrak{G}(\mathbf{X}, \mathbf{Y})$ is the symmetric bilinear form associated with $\mathfrak{G}(\mathbf{X})$ and where $\mathbf{e}_1, \dots, \mathbf{e}_m$ are the basis vectors. Given a quadratic form $\mathfrak{F}(X_1, \dots, X_n)$, suppose we have linearly independent vectors $\mathbf{x}_1, \dots, \mathbf{x}_m$ with

$$\mathfrak{F}(\mathbf{x}_i, \mathbf{x}_j) = 0 \qquad (1 \le i < j \le m). \tag{6.1}$$

Let $T\colon \mathbf{Q}^m \to \mathbf{Q}^n$ be the linear map with $T\mathbf{e}_i = \mathbf{x}_i$ $(i = 1, \dots, m)$. Then the form $\mathfrak{G}(\mathbf{Y}) = \mathfrak{F}(T\mathbf{Y})$ is diagonal; we say that $\mathfrak{G}$ is *represented* by $\mathfrak{F}$.

LEMMA 2. *Suppose that $n \geq 4m$. Let $\mathfrak{F}(X_1, \ldots, X_n)$ be a quadratic form with rational integer coefficients. Then there are linearly independent integer points $\mathbf{x}_1, \ldots, \mathbf{x}_m$ with* (6.1) *and with*

$$|\mathbf{x}_j| \ll F^{4m/n} \qquad (j = 1, \ldots, m). \tag{6.2}$$

PROOF. Set $\mathbf{x}_1 = \mathbf{e}_1$. Suppose $k < m$, and $\mathbf{x}_1, \ldots, \mathbf{x}_k$ have already been constructed with (6.1), (6.2) holding for $j \leq k$. We may suppose without loss of generality that the projections of these k points on the space spanned by the first k coordinate axes are independent. Consider the linear forms $\mathfrak{L}_i(\mathbf{X}) = \mathfrak{F}(\mathbf{x}_i, \mathbf{X})$ $(i = 1, \ldots, k)$ in vectors $\mathbf{X} = (0, \ldots, 0, X_{k+1}, \ldots, X_n)$. We note that $|\mathfrak{L}_i| \ll F|\mathbf{x}_i| \ll F^2$. Applying Siegel's Lemma with $l = n - k$ we obtain a nontrivial integer zero of $\mathfrak{L}_1, \ldots, \mathfrak{L}_k$, call it $\mathbf{x}_{k+1}$, with

$$|\mathbf{x}_{k+1}| \ll F^{2k/(n-2k)} \leq F^{2m/(n-2m)} \leq F^{4m/n}.$$

Now in order to prove Theorem 4 when $n \geq 40$, we choose $k > 0$ with

$$8k(4k+1) \leq n \tag{6.3}$$

and we set $m = 4k+1$. We apply Lemma 2 and we set $a_i = \mathfrak{F}(\mathbf{x}_i, \mathbf{x}_i)$ $(i = 1, \ldots, m)$. If some $a_i = 0$, then $\mathbf{x}_i$ is a zero of $\mathfrak{F}$ with $q_p(\mathbf{x}_i) \leq |\mathbf{x}_i| \ll F^{4m/n} \leq F^{1/2k}$ and we are done.

We may thus suppose that each $a_i \neq 0$. We have $|a_i| \ll F^{1+8m/n} \leq F^{1+1/k} \leq F^2$ and therefore $1 \geq |a_i|_p \gg F^{-2}$. Recalling that $m = 4k+1$ and reordering we have

$$1 \geq |a_1|_p \geq \cdots \geq |a_5|_p \geq \cdots \geq |a_9|_p \geq \cdots \geq |a_{4k+1}|_p \gg F^{-2}.$$

There is some t with

$$|a_{4t+1}|_p \geq \cdots \geq |a_{4t+5}|_p \gg F^{-2/k}|a_{4t+1}|_p.$$

Reordering again if necessary we may suppose that

$$|a_i/a_j|_p \ll F^{2/k} \qquad (1 \leq i,\ j \leq 5). \tag{6.4}$$

The linear map $T\colon \mathbf{Q}^5 \to \mathbf{Q}^n$ with $T\mathbf{e}_i = \mathbf{x}_i$ $(i = 1, \ldots, 5)$ has norm $|T| \ll F^{4m/n} \leq F^{1/2k}$ and transforms $\mathfrak{F}$ into the diagonal form $\mathfrak{F}(T\mathbf{Y}) = a_1Y_1^2 + \cdots + a_5Y_5^2$. We have

$$T\mathbf{Y} = (\mathfrak{M}_1(\mathbf{Y}), \ldots, \mathfrak{M}_n(\mathbf{Y})) \tag{6.5}$$

with linear forms $\mathfrak{M}_i$ having coefficients in $\mathbf{Z}$ and of norm $|\mathfrak{M}_i| \ll |T| \ll F^{1/2k}$.

PROPOSITION 3. *Let $\mathfrak{G} = a_1Y_1^2 + \cdots + a_5Y_5^2$ be a form with nonzero coefficients in $\mathbf{Q}$ having*

$$|a_i/a_j|_p \leq B_1 \qquad (1 \leq i,\ j \leq 5). \tag{6.6}$$

Let $\mathfrak{M}_1, \ldots, \mathfrak{M}_n$ be linear forms in $\mathbf{Y} = (Y_1, \ldots, Y_5)$ whose coefficients c_{it} $(1 \leq i \leq n,\ 1 \leq t \leq 5)$ are integers, and each coefficient $c_{it} = 0$ or it has $|c_{it}|_p \geq B_2^{-1}$.

Then $\mathfrak{G}$ has a zero $\mathbf{y} \in \mathbf{Z}^5 \backslash \mathbf{0}$ such that each $\mathfrak{M}_i(\mathbf{y})$ is either zero or has

$$|\mathfrak{M}_i(\mathbf{y})|_p \gg B_1^{-1/2}B_2^{-1}. \tag{6.7}$$

The constant in $\gg$ depends only on n, p.

If we apply the proposition to the forms $\mathfrak{M}_i$ in (6.5) and with $B_1 \ll F^{2/k}$, $B_2 \ll F^{1/2k}$, we obtain $\mathbf{x} = T\mathbf{y} \neq \mathbf{0}$ with $\mathfrak{F}(\mathbf{x}) = \mathfrak{G}(\mathbf{y}) = 0$ and $q_p(\mathbf{x}) \ll B_1^{1/2}B_2 \ll$

$F^{3/2k}$. Hence Theorem 4 with $c_n = 3/2k$ will follow once we have proved Proposition 3. (As was pointed out in the introduction, Theorem 4 with $c_n = 4$ is a consequence of Theorem 5, which will be proved in §8.)

7. A counting argument. Let v be the "valuation" with $|a|_p = p^{-v(a)}$. Replacing $\mathfrak{G}$ by a proportional form if necessary, we may suppose that

$$\max(v(a_1), \dots, v(a_5)) = 0.$$

Then $1 \le |a_i|_p \le B_1$ by (6.6). We write $v(a_i) = -2e_i + \varepsilon_i$ where $\varepsilon_i = 0$ or 1, so that $p^{2e_i - \varepsilon_i} \le B_1$ and $p^{e_i} \ll B_1^{1/2}$ $(i = 1, \dots, 5)$. With the substitution $Y_i = p^{e_i} Z_i$, the form $\mathfrak{G}(\mathbf{Y})$ becomes

$$\mathfrak{H}(\mathbf{Z}) = b_1 Z_1^2 + \cdots + b_5 Z_5^2,$$

where $v(b_i) = \varepsilon_i$. After multiplying $\mathfrak{H}$ by a suitable rational number, we may suppose that $b_1, \dots, b_5$ are rational integers and are not divisible by p^2. Further $\mathfrak{M}_i(\mathbf{Y}) = \mathfrak{N}_i(\mathbf{Z})$, where the linear forms $\mathfrak{N}_i$ have coefficients d_{it} in $\mathbf{Z}$ $(1 \le i \le n,\ 1 \le t \le 5)$, and each d_{it} is either zero or has

$$|d_{it}|_p \gg B_2^{-1} B_1^{-1/2} = B^{-1}, \tag{7.1}$$

say.

LEMMA 3. *The form $\mathfrak{H}$ has a zero $\mathbf{w} \in \mathbf{Z}^5$ with*

$$p^4 \nmid w_i \qquad (i = 1, \dots, 5). \tag{7.2}$$

PROOF. $\mathfrak{H}$ has a p-adic zero $\mathbf{x}$, and hence the congruence $\mathfrak{H}(\mathbf{x}) \equiv 0 \pmod{p^6}$ has a primitive solution $\mathbf{x} = (x_1, \dots, x_5)$ with $\gcd(p, x_1, \dots, x_5) = 1$. Suppose that $p \nmid x_1$. Let $\mathbf{y} = (y_1, \dots, y_5)$, where $y_i = x_i$ when $p^4 \nmid x_i$ and $y_i = p^3$ when $p^4 | x_i$. Then again $\mathfrak{H}(\mathbf{y}) \equiv 0 \pmod{p^6}$, and further $p^4 \nmid y_i$ $(i = 1, \dots, 5)$. Further $\partial \mathfrak{H} / \partial y_1 \not\equiv 0 \pmod{p^3}$, since $p^2 \nmid b_1$ and $p \nmid y_1 = x_1$. (Some exponents could be lowered for $p \ne 2$.) By Hensel's Lemma (see e.g., [**5**, p. 14, Theorem 1] with[4] $0 \le k \le 2$, $n = 6$), the form $\mathfrak{H}$ has a p-adic zero $\mathbf{z} \equiv \mathbf{y} \pmod{p^4}$. This zero has $1 \ge |z_i|_p \ge p^{-3}$ $(i = 1, \dots, 5)$. Since the rational zeros of $\mathfrak{H}$ are "dense" in the set of p-adic zeros, there is a rational zero, hence a rational integer zero $\mathbf{w}$ with $|w_i|_p = |z_i|_p \ge p^{-3}$.

Set

$$\mathbf{z}(\mathbf{X}) = 2\mathfrak{H}(\mathbf{w}, \mathbf{X})\mathbf{X} - \mathfrak{H}(\mathbf{X})\mathbf{w}, \tag{7.3}$$

where $\mathbf{X} = (X_1, \dots, X_5)$. Then $\mathfrak{H}(\mathbf{z}(\mathbf{X}))$ vanishes identically, and $\mathbf{x} \mapsto \mathbf{z}(\mathbf{x})$ maps $\mathbf{Z}^5 \to \mathbf{Z}^5$. We will show that "many" integer points $\mathbf{x}$ are such that the $\mathfrak{N}_i(\mathbf{z}(\mathbf{x}))$ $(i = 1, \dots, n)$ have the right property, i.e., each is either zero or has

$$|\mathfrak{N}_i(\mathbf{z}(\mathbf{x}))|_p \gg B^{-1}. \tag{7.4}$$

Assuming that $\mathfrak{N}_1, \dots, \mathfrak{N}_t$ are those forms $\mathfrak{N}_i$ which do not vanish identically, we will construct $\mathbf{x}$ such that (7.4) holds for $i = 1, \dots, t$. Now

$$\mathfrak{N}_i(\mathbf{z}(\mathbf{X})) = 2\mathfrak{H}(\mathbf{w}, \mathbf{X})\mathfrak{N}_i(\mathbf{X}) - \mathfrak{H}(\mathbf{X})\mathfrak{N}_i(\mathbf{w}) = \mathfrak{E}_i(\mathbf{X}),$$

say.

[4] The condition $0 \le 2k$ in [**5**] should read $0 < 2k$.

LEMMA 4. *Each quadratic form* $\mathfrak{E}_i(\mathbf{X})$ $(i = 1, \dots, t)$ *has some coefficient with p-adic absolute value* $\gg B^{-1}$.

PROOF. Keep i fixed at the moment. In $\mathfrak{N}_i(\mathbf{X}) = d_1X_1 + \cdots + d_5X_5$ we may suppose that $d_1 \neq 0$, so that $|d_1|_p \gg B^{-1}$ by (7.1). Since $\mathfrak{H}$ is diagonal, it will be enough to show that the coefficient of one of the mixed terms X_1X_2, X_1X_3, X_2X_3 of $2\mathfrak{H}(\mathbf{w}, \mathbf{X})\mathfrak{M}_i(\mathbf{X})$ has p-adic absolute value $\gg B^{-1}$. Writing μ for the maximum value of these three coefficients, we have

$$|b_1w_1d_2 + b_2w_2d_1|_p \leq \mu, \quad |b_1w_1d_3 + b_3w_3d_1|_p \leq \mu, \quad |b_2w_2d_3 + b_3w_3d_2|_p \leq \mu.$$

Multiplying respectively by $b_3w_3, b_2w_2, -b_1w_1$ we obtain $|2b_2w_2b_3w_3d_1|_p \leq \mu$. Since $|b_i|_p \geq p^{-1}$ and by (7.2), we have $\mu \gg |d_1|_p \gg B^{-1}$.

LEMMA 5. *Let* $\mathfrak{E}(\mathbf{X})$ *be a quadratic form in s variables with coefficients in* $\mathbf{Z}$, *and with at least one coefficient not divisible by* p^{v+1}. *Then as* $\mathbf{x} = (x_1, \dots, x_s)$ *runs through a complete set of vectors modulo* p^{2m}, *the number of* $\mathbf{x}$ *with* $\mathfrak{E}(\mathbf{x}) \equiv 0 \pmod{p^{v+2m}}$ *is* $\ll p^{2ml-m}$. *The constant in* $\ll$ *may depend on s and p, but it is independent of v and m.*

This is essentially Lemma 16 of [**4**]. The reader may prefer to find his own simple proof.

The proof of Proposition 3 is now completed by a counting argument. Let v be smallest possible such that each of $\mathfrak{E}_1, \dots, \mathfrak{E}_t$ has a coefficient of p-adic absolute value $\geq p^{-v}$. Then $p^v \ll B$ by Lemma 4. Therefore by Lemma 5 the number of $\mathbf{x} = (x_1, \dots, x_5)$ modulo p^{2m} for which at least one of

$$\mathfrak{E}_i(\mathbf{x}) \equiv 0 \pmod{p^{v+2m}} \qquad (i = 1, \dots, t)$$

holds is $\ll tp^{9m} \ll p^{9m}$, with a constant in $\ll$ depending only on n, p. So when $m \geq m_0(n, p)$, this number is less than p^{10m}. Thus there is an $\mathbf{x}$ with $\mathfrak{E}_i(\mathbf{x}) \not\equiv 0 \pmod{p^{v+2m_0}}$ $(i = 1, \dots, t)$. But this gives

$$|\mathfrak{E}_i(\mathbf{x})|_p > p^{-v-2m_0} \gg p^{-v} \gg B \qquad (i = 1, \dots, t).$$

8. Proof of Theorem 5. By hypothesis (c) we may suppose without loss of generality that $\mathfrak{F}$ has a zero $\mathbf{w} = (w_1, \dots, w_n)$ with $1 = |w_1| \geq \cdots \geq |w_n|$. In analogy to (7.3) set

$$\mathbf{z}(\mathbf{X}) = 2\mathfrak{F}(\mathbf{w}, \mathbf{X})\mathbf{X} - \mathfrak{F}(\mathbf{X})\mathbf{w}.$$

Then $\mathfrak{F}(\mathbf{z}(\mathbf{X}))$ vanishes identically. We have

$$\mathbf{z}(\mathbf{X}) = (z_1(\mathbf{X}), \dots, z_n(\mathbf{X})),$$

where each z_t is a quadratic form. Since each $|f_{ij}| \leq 1$ and each $|w_i| \leq 1$, the coefficients of z_t also have absolute value ≤ 1.

LEMMA 6. *Each form* z_t *has a coefficient of absolute value* $\geq B^{-1}$.

PROOF. Denote the maximum absolute value of the coefficients of z_t by μ_t. In $z_t = 2\mathfrak{F}(\mathbf{w}, \mathbf{X})X_t - \mathfrak{F}(\mathbf{X})w_t$, the coefficient c_{tj} of $2c_{tj}X_tX_j$ with $j \neq t$ is

$$c_{tj} = \mathfrak{F}(\mathbf{w}, \mathbf{e}_j) - \mathfrak{F}(\mathbf{e}_t, \mathbf{e}_j)w_t = \mathfrak{F}(\mathbf{w}_t, \mathbf{e}_j)$$

with $\mathbf{w}_t = \mathbf{w} - w_t\mathbf{e}_t = (w_1, \dots, w_{t-1}, 0, w_{t+1}, \dots, w_n)$. So

$$\left|\sum_{l\neq t} f_{lj}w_l\right| = |\mathfrak{F}(\mathbf{w}_t, \mathbf{e}_j)| \leq \mu_t \qquad (j \neq t). \tag{8.1}$$

Let $\mathfrak{A}^t$ be the $(n-1)\times(n-1)$-matrix (f_{lj}) with $l \neq t$, $j \neq t$, and let A^t_{kj} be the cofactor of f_{kj} in $\mathfrak{A}^t$. We multiply (8.1) by A^t_{kj} and take the sum over $j \neq t$. Since $|A^t_{kj}| \leq 1$ and since

$$\sum_{j\neq t} f_{lj}A^t_{kj} = \delta_{lk}\det\mathfrak{A}^t = \delta_{lk}A_{tt}$$

with the Kronecker symbol δ_{lk}, it follows that

$$|A_{tt}w_k| \leq \mu_t \qquad (k \neq t).$$

When $t \neq 1$, we may take $k = 1$ and we get $\mu_t \geq |A_{tt}| \geq B^{-1}$. On the other hand when $t = 1$, we note that the coefficient of X_n^2 in $z_1(\mathbf{X})$ equals $-f_{nn}w_1$, so that $\mu_1 \geq |f_{nn}| \geq B^{-1}$.

In the case when $K = \mathbf{Q}$ or $\mathbf{Q}_p$ with the p-adic absolute value we apply Lemma 5 and see that for a "positive proportion" of $\mathbf{x} \in \mathbf{Z}^n$ we have $|z_i(\mathbf{X})| \gg B^{-1}$ $(i = 1, \dots, n)$. In general one has to use a suitable analogue of Lemma 5.

REFERENCES

1. J. W. S. Cassels, *Bounds for the least solutions of homogeneous quadratic equations,* Proc. Cambridge Philos. Soc. **51** (1955), 262–264.
2. ——, *Addendum to "Bounds for the least solutions of homogeneous quadratic equations"*, Proc. Cambridge Philos. Soc. **52** (1956), 604.
3. H. P. Schlickewei, *Kleine Nullstellen homogener quadratischer Gleichungen* (in preparation).
4. W. M. Schmidt, *On cubic polynomials. II. Multiple exponential sums,* Monatsh. Math. **93** (1982), 141–168.
5. J. P. Serre, *A course in arithmetic*, Graduate Texts in Math., vol. 7, Springer, New York and Berlin, 1973.
6. G. L. Watson, *Least solutions of homogeneous quadratic equations,* Proc. Cambridge Philos. Soc. **53** (156), 541–543.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF COLORADO, BOULDER, COLORADO 80309