with \( b = w, l = r + 1^2 + 2^2 + \cdots + (n-1)^2 \) and \( q = s \). For the second statement one can apply the Corollary of [6], Theorem 3 with \( a_i = n, b_i = i, c_i = d_i = r + 1^2 + 2^2 + \cdots + (n-1)^2 \).

Added in proof. A result similar to Theorem 1, but for the equation \( 1^2 + 2^2 + \cdots + n^2 + R(x) = y^2 \), has been published in Acta Math. 143 (1979), pp. 1-3.

Here \( R \) is a fixed polynomial with rational integer coefficients. The proof in that paper differs from the proof in this paper. Furthermore, a proof of the result of Stroeker mentioned in Remark 1 has been published in Nieuw Arch. Wiskunde 24 (1978), pp. 470-478.

References


Received on 19. 10. 1977

---

Small solutions of quadratic congruences and small fractional parts of quadratic forms

by A. SCHINZEL (Warszawa), H. P. SCHLICKEWI and W. M. SCHMIDT* (Boulder, Colo.)

1. Introduction. As for quadratic congruence, we have

Theorem 1. Let \( Q(x) = Q(x_1, \ldots, x_k) \) be a quadratic form with integer coefficients in an odd number \( h \) of variables. Then for each natural \( m \) there are integers \( x_1, \ldots, x_k \) satisfying

\[
Q(x_1, \ldots, x_k) \equiv 0 \pmod{m}
\]

and having

\[
0 < \max(|x_1|, \ldots, |x_k|) \leq m^{(h)}
\]

where \( m^{(h)} = (1/h) + (1/2h) \).

It is clear that the result remains valid for even \( h \), provided we set \( m^{(h)} = ((1/2) + (1/2(h-1))) \) in this case. Clearly \( m^{(h)} \) may not be replaced by a number less than \( 1/2 \), but it is conceivable that the theorem remains true with the right hand side of (2) replaced by \( cm^{(h)} \) for \( h \gg h_0 \).

As for fractional parts, Heilbronn [1] proved that for \( s > 0 \), \( N > c_s(s) \) and arbitrary real \( a \), there exists a natural \( n \leq N \) with

\[
|an|^s < N^{(-1/s)+}\]

where \( |.| \) denotes the distance to the nearest integer. Danicic [2] generalized Heilbronn's result by showing that for \( s > 0 \), \( N > d_s(s, s) \) and a quadratic form \( Q(x_1, \ldots, x_k) \), there exist integers \( n_1, \ldots, n_k \) not all zero, with \( |n_1|, \ldots, |n_k| \leq N \) and with

\[
|Q(n_1, \ldots, n_k)| < N^{-(s/((s+1)))}\]

Cook [1] was able to show that for \( s > 0 \), \( N > c_s(s) \) and arbitrary \( a_1, a_2 \), there exist integers \( n_1, n_2 \) not both zero, having \( |n_1|, |n_2| \leq N \) and

\[
|a_1n_1 + a_2n_2| < N^{-1/s}.
\]

* Written while the second author had a research fellowship from the Max Kade Foundation, New York.

---

26 — Acta Arithmetica XXXVII
For $s \geq 1$, let $c_q(s)$ be the maximum of
\[ 2 \left( \frac{1 + \frac{1}{h} + \frac{4}{s - h + 1}}{s - h + 1} \right) \]
over odd $h$ in $1 \leq h \leq (s + 5)/3$. Taking $h$ asymptotically equal to $s/3$ we obtain $c_q(s) = 2 - (18/5) + O(1/s^3)$.

**Theorem 2.** Let $s \geq 1$, $c > 0$, $N > c_q(s)$, and let $Q(x_1, \ldots, x_s)$ be a quadratic form. Then there are integers $n_1, \ldots, n_s$ with
\[ 0 < \max(|n_1|, \ldots, |n_s|) \leq N \]
having
\[ \|Q(n_1, \ldots, n_s)\| < N^{-c_1(s)^{1/2}} \]  

For $s \leq 5$, the result of Davenport is stronger than ours, for $s = 6$ we get the same exponent as Davenport, and for $s > 7$ our exponent is better. That the constant $c_q(s)$ may not be replaced by a number greater than 2 is seen by taking the special quadratic form $\alpha x_1^2 + \cdots + x_s^2$ where $\alpha$ is a number with bounded partial denominators in its continued fraction. However, it is conceivable that the theorem remains true with $c_q(s)$ replaced by 2 for $s > 7$. For many special quadratic forms, $c_q(s)$ may be replaced by a number much larger than 2 (Schmidt [5]).

We will make use of Theorem 1 in order to prove Theorem 2. On the other hand, given an integral form $Q(x) = Q(x_1, \ldots, x_s)$, and applying Theorem 2 to $Q_1(x) = m^{-1}Q(x)$ and $N = m^{-1}Q_1(-m)$, we note the existence of a solution of (1) with $0 < \max(|x_1|, \ldots, |x_s|) \leq N$, so that Theorem 1 holds with $e(k) = 1/(n(k) - c)$, provided that $m$ is large. Hence Theorem 1 may be regarded as a discrete version of Theorem 2.

No analogous results are known for degrees of greater than 2. But for diagonal forms, see Schmidt [5].

### 2. Congruences

**Lemma 1.** Let $Q(x) = Q(x_1, \ldots, x_s)$ be a quadratic form with coefficients in the finite field $\mathbb{F}_q$ with $q$ elements. Then $Q$ vanishes on a certain subspace $S$ of $h$-dimensional space $\mathbb{F}_q^h$ of dimension $[(h-1)/2]$ (where $[ \cdot ]$ denotes the integer part).

**Proof.** Much more was shown by Segre [7]. A simple proof is as follows. We may suppose that $h \geq 3$, that $h$ is odd and that $Q$ is nonsingular.

Suppose at first that $q$ is odd. Then $Q$ is equivalent to a form
\[ y_1y_2 + y_2y_3 + \cdots + y_{h-2}y_{h-1} + a y_h^2, \]
and we may take $S$ to be the subspace with $y_1 = y_2 = \cdots = y_{h-2} = y_h = 0$.

On the other hand, if $q$ is even, the form may be seen to be equivalent to a form
\[ a y_1^2 + \cdots + a y_s^2 + a y_1y_i + a y_2y_i + \cdots + a y_{h-1}y_h. \]

In this case we define $S$ by $a y_1 + \cdots + a y_s y_s = 0$ and $y_s = y_2 = \cdots = y_{h-1} = 0$.

**Proof of Theorem 1.** If $m = \omega q_1$ and if $y_1, \ldots, y_s$ satisfy $Q(y_1, \ldots, y_s) = 0$ (mod $m_1$) and $0 < \max(|y_1|, \ldots, |y_s|) \leq m_1^{(s)}$, then $x_1 = y_1, \ldots, x_s = y_s$ will satisfy (1) and (2). Hence we may suppose $m$ to be square free. Of course we may suppose that $m > 1$ and $h > 1$. Observe that $k$ is odd by hypothesis, and put $d = (h-1)/2$.

For every prime $p$ dividing $m$, there are by Lemma 1 integer points $v_{1p}, \ldots, v_{dp}$ which are linearly independent modulo $p$ and such that $Q(x) = 0$ (mod $p$) for each combination $x = v_{1p} + \cdots + a v_{dp}$ with integer coefficients. By the Chinese Remainder Theorem there are integer vectors $v_1, \ldots, v_d$ having $v_i = v_{ip}$ (mod $p$) for each prime factor $p$ of $m$. Write $v_i = (v_{1i}, \ldots, v_{di})$. We have $Q(x) \equiv 0$ (mod $m$) for
\[ x = v_1 + \cdots + a v_d + m x \]
with integers $a_1, \ldots, a_d$ and with $x = (x_1, \ldots, x_d)$ integral. According to Minkowski's Linear Forms Theorem, there are integers $a_1, \ldots, a_d, x_1, \ldots, x_h$, not all zero, with
\[ |c_i| < m \quad (i = 1, \ldots, d), \]
\[ |a_1 v_1 + \cdots + a_d v_d + m x| < m^{1/2} (m^h) \quad (j = 1, \ldots, h). \]
The vector $x = (x_1, \ldots, x_s)$ given by (6) satisfies (1) and $\max(|x_1|, \ldots, |x_s|) \leq m^{s/2}$. If $a_1 = \cdots = a_d = 0$, then also $x_1 = \cdots = x_h = 0$, which is impossible. If, say, $a_1 \neq 0$, then by (7) there is a prime factor $p$ of $m$ with $c_1 \neq 0$ (mod $p$). In view of the linear independence of $v_1, \ldots, v_d$ modulo $p$, we have $x \equiv 0$ (mod $p$), whence $x \equiv 0$.

### 3. An Alternative Lemma

We now turn to Theorem 2. So let
\[ Q(x) = Q(x_1, \ldots, x_h) = \sum_{i,j} \lambda_{ij} x_i x_j \]
be a quadratic form with real coefficients. The matrix $(\lambda_{ij})$ may be supposed to be symmetric. We have
\[ Q(x) = \lambda_1 L_1(x) + \cdots + \lambda_s L_s(x) \]
where $L_i(x) = \lambda_i x_1^2 + \cdots + \lambda_i x_i$ (i = 1, \ldots, s).

The symbol $[\ldots]$ will denote fractional parts: $[a] = a - [a]$.  

**Lemma 2 (Alternative Lemma).** Let $1 > \varepsilon > 0, s > 1, N > c_q(\varepsilon s)$ and $N^{-c^{1+\varepsilon}} \leq 1 < 1$. Then either
Small solutions of quadratic congruences

\[ ||Q(n_1, \ldots, n_s)|| = ||Q(r_{11}x_1 + \ldots + r_{1h}x_h, \ldots, r_{s1}x_1 + \ldots + r_{sh}x_h)|| \]
\[ = \left| \frac{1}{m} \sum_{\mu=1}^{h} \sum_{\nu=1}^{h} \varphi_{\mu\nu}^x \varphi_{\mu\nu}^y \right| \]
\[ \leq \frac{1}{m} \sum_{\mu=1}^{h} \sum_{\nu=1}^{h} \left| \varphi_{\mu\nu}^x \right| \left| \varphi_{\mu\nu}^y \right| \]

From (12), (9), (10) and since \( |x_j| \leq m^{\varepsilon(h)} \) \((1 \leq \mu \leq h)\), we get
\[ ||Q(n_1, \ldots, n_h)|| \leq s^2 m^{2\varepsilon(h)-1} (I^{-h(\frac{\varepsilon(h)}{2}+1)}) \]
\[ N^{\varepsilon(h)} - N^{-2(h-1)} N^{\varepsilon(h)-1} \]

By virtue of (8) and of \( 2\varepsilon(h) - 1 = 1/h \), this is
\[ \leq s^2 \left( I^{-h(\frac{\varepsilon(h)}{2}+1)} \right) N^{\varepsilon(h)-2} \]
and for large \( N \) it is
\[ < N^{\varepsilon(h)-O((1/3)+(1/3-h+1))} N^{-2} < N^{-\varepsilon(h)+1} \]

4. Davenport's Lemma

Lemma 3. Let \( L_1, \ldots, L_s \) be real linear forms in \( x = (x_1, \ldots, x_h) \) and with a symmetric coefficient matrix. Let \( N \geq 1 \) and let \( M_1, \ldots, M_s \) be the first \( s \) successive minima of the convex body described by
\[ |L_j(x)| < m^{\varepsilon(h)} \] \((j = 1, \ldots, s)\)
\[ |x_j| < N \]
with respect to the lattice of integer points in 2\( h \)-dimensional space. Then the number of integer points \( x = (x_1, \ldots, x_h) \) satisfying the simultaneous inequalities
\[ ||L_j(x)|| < m^{\varepsilon(h)} \] \((j = 1, \ldots, s)\)
\[ |x_j| < N \]
is \( \ll (M_1 \cdots M_s)^{-1} \).

Here and in the sequel the constant implied by \( \ll \) depends only on \( s \) and \( e \).

This is Lemma 3 of Davenport [3]. Put
\[ \mathcal{S}(k) = \sum_{(n_1, \ldots, n_h) \in \mathcal{Q}} e(hQ(n_1, \ldots, n_h)), \]
where \( e(\cdot) = e^{2\pi i \cdot} \), \( k \) is natural and \( \mathcal{Q} \) is the set given by (4).

Lemma 4 (Davenport's Alternative Lemma). Suppose that \( 1 \leq h < s \) and
\[ Z \gg \alpha(\varepsilon(\mathcal{Q}(h-1))) \]

On the other hand, by (11)}
which contradicts the linear independence of $R_1, \ldots, R_h$. As a consequence, we obtain alternative (ii).

Now suppose that $M_h \geq Z^{-1}$. Let $\nu$ be the number of integer solutions $(x_1, \ldots, x_h)$ of the simultaneous inequalities

$$||2kL_j(x_1, \ldots, x_h)|| < N^{-1} \quad (j = 1, \ldots, \nu)$$

$$|x_j| < N$$

It is well known that

$$|S(k)|^2 \leq \nu N^2 (\log N)^4$$

(cf. Davenport [3], p. 117). By Lemma 3 we have

$$\nu \ll (M_1 \ldots M_h)^{-1}.$$  

Notice that $M_1 \gg N^{-1}$; this follows from the definition of the convex body (14). With (19) and $M_h \gg Z^{-1}$ we infer that

$$\nu \ll N^{k-1}Z^{-k+1}.$$  

By virtue of (18), this implies (i).

5. **Proof of the Alternative Lemma.** Suppose that the first alternative in Lemma 2 does not hold. There is an interval $S$ of length $I$, such that $Q(a_1, \ldots, a_h) \notin S$ for $h$-tuples $(a_1, \ldots, a_h)$ in the set $\mathfrak{K}$ given by (4). Choose $r > 1 + 10e^{-7}$. By a lemma of Vinogradov ([8], Lemma 12; or see [6], § 3), there is a function $\varphi(a)$, periodic with period $1$, having $\varphi(x) = 0$ unless $x$ lies in an integer translate of $S$, and having a Fourier expansion

$$\varphi(x) = \frac{1}{I} + \sum_{q \neq 0} \frac{\sigma(q) \varphi(q)}{q}$$

where

$$|\varphi_q| \ll I \min \{1, (qI)^{-r}\}.$$  

We have

$$\sum_{(a_1, \ldots, a_h) \in S} \varphi(Q(a_1, \ldots, a_h)) = 0.$$  

The Fourier expansion of $\varphi$ yields

$$\sum_{q \neq 0} |\varphi_q| |S(q)| \ll N^r I.$$  

Setting $K = [I^{-1}N^{10}]$ we obtain

$$\sum_{|q| \leq K} |\varphi_q| |S(q)| \ll N^r \sum_{|q| \leq K} |\varphi_q| \ll N^r I \sum_{q \leq K} (qI)^{-r}$$

$$\ll N^r (IK)^{-r} \ll N^r (\log I)^{r-1} \ll o(N^r I),$$

for $r > 1$. Hence, $\varphi(x) = 0$ for all $x$ in $[0, I]$ except at most $O(N^r I)$ points. Therefore, $S$ cannot be a union of several intervals of length $I$, and the conclusion follows.
by our choice of $r$. Thus from (20), and since $|c| < I$ and $|S(q)| = |S(-q)|$, we have
\[
\sum_{q=1}^{K} |S(q)| \gg N^r.
\]
Hence there is a $q_0$, $1 \leq q_0 \leq K \leq I^{-1}N^{10}$, with
\[
|S(q_0)|^2 \gg N^{2s}K^{-1}.
\]
Now let $h$ be odd with $1 \leq h \leq (s+5)/3$. Then by the lower bound for $I$ in the hypothesis of Lemma 2, the inequality (13) holds for
\[
Z = N^{1-(4(s-4)/3)}T^{4/3-\frac{4}{3}h-1}.
\]
With this choice of $Z$ we have
\[
Z^{-3/4}N^{s-1/4} \log N \leq N^{2s-4}T^{4/3}N^{4/3} = N^{2s-4}T^{4/3}N^{4/3} \leq N^{2s}K^{-1},
\]
by the definition of $K$, if $N$ is large enough. Hence by (21) the second alternative of Lemma 4 holds with $k = q_0$. This implies the second alternative of Lemma 2 with $m = 2q_0 = 2k$ for $N$ large enough.

References


POLISH ACADEMY OF SCIENCES, WROCŁAW
UNIVERSITY OF COLORADO AND MATH. INST. UNIV. FREIBURG
UNIVERSITY OF COLORADO, BOLDER

Received on 21. 10. 1977 (992)