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

Added in proof. A result similar to Theorem 1, but for the equation $1^k+2^k+\ldots+x^k+R(x) = y^z$, has been published in Acta Math. 143 (1979), pp. 1–8. 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. 476–478.

References

[1] A. Baker, *Bounds for the solutions of the hyperelliptic equation*, Proc. Cambridge Philos. Soc. 65 (1969), pp. 439–444.

[2] J. Brillhart, *On the Euler and Bernoulli polynomials*, J. Reine Angew. Math. 234 (1969), pp. 45–64.

[3] H. Rademacher, *Topics in analytic number theory*, Springer Verlag, Berlin 1973.

[4] J. J. Schäffer, *The equation* $1^p+2^p+3^p+\ldots+n^p = m^q$, Acta Math. 95 (1956), pp. 155–189.

[5] T. N. Shorey, A. J. van der Poorten, R. Tijdeman and A. Schinzel, *Applications of the Gel'fond–Baker method to Diophantine equations*, in: *Transcendence Theory: Advances and applications*, Academic Press, London 1979, pp. 59–77.

[6] T. N. Shorey and R. Tijdeman, *New applications of Diophantine approximations to Diophantine equations*, Math. Scand. 39 (1976), pp. 5–18.

MATHEMATICAL INSTITUTE
KOSSUTH LAJOS UNIVERSITY
4010 Debrecen, Hungary

MATHEMATICAL INSTITUTE
Leiden, The Netherlands

MATHEMATICAL CENTRE
Amsterdam, The Netherlands

Received on 19. 10. 1977 (991)

ACTA ARITHMETICA
XXXVII (1980)

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

by

A. Schinzel (Warszawa), H. P. Schlickewei and W. M. Schmidt* (Boulder, Colo.)

1. Introduction. As for quadratic congruence, we have

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

$$Q(x_1, \ldots, x_h) \equiv 0 \pmod m \tag{1}$$

and having

$$0 < \max(|x_1|, \ldots, |x_h|) \leqslant m^{e(h)}, \tag{2}$$

where $e(h) = (1/2)+(1/2h)$.

It is clear that the result remains valid for even h, provided we set $e(h) = (1/2)+\big(1/2(h-1)\big)$ in this case. Clearly $e(h)$ 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 $c_0 m^{1/2}$ for $h \geqslant h_0$.

As for fractional parts, Heilbronn [4] proved that *for* $\varepsilon > 0$, $N > c_1(\varepsilon)$ *and arbitrary real* α, *there exists a natural* $n \leqslant N$ *with*

$$\|\alpha n^2\| < N^{-(1/2)+\varepsilon}$$

where $\|\ldots\|$ denotes the distance to the nearest integer. Danicic [2] generalized Heilbronn's result by showing that *for* $\varepsilon > 0$, $N > c_2(\varepsilon, s)$ *and a quadratic form* $Q(x_1, \ldots, x_s)$, *there exist integers* $n_1, \ldots, n_s$ *not all zero, with* $|n_1|, \ldots, |n_s| \leqslant N$ *and with*

$$\|Q(n_1, \ldots, n_s)\| < N^{-(s/(s+1))+\varepsilon}.$$

Cook [1] was able to show that *for* $\varepsilon > 0$, $N > c_3(\varepsilon)$ *and arbitrary* α_1, α_2, *there exist integers* n_1, n_2 *not both zero, having* $|n_1|, |n_2| \leqslant N$ *and*

$$\|\alpha_1 n_1^2+\alpha_2 n_2^2\| < N^{-1+\varepsilon}.$$

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

For $s \geqslant 1$, let $c_4(s)$ be the maximum of

$$2\left(1+\frac{1}{h}+\frac{4}{s-h+1}\right)^{-1} \tag{3}$$

over odd h in $1 \leqslant h \leqslant (s+5)/3$. Taking h asymptotically equal to $s/3$ we obtain $c_4(s) = 2-(18/s)+O(1/s^2)$.

THEOREM 2. *Let $s \geqslant 1$, $\varepsilon > 0$, $N > c_5(\varepsilon, s)$, and let $Q(x_1, \ldots, x_s)$ be a quadratic form. Then there are integers $n_1, \ldots, n_s$ with*

$$0 < \max(|n_1|, \ldots, |n_s|) \leqslant N \tag{4}$$

having

$$\|Q(n_1, \ldots, n_s)\| < N^{-c_4(s)+\varepsilon}. \tag{5}$$

For $s \leqslant 5$, the result of Danicic is stronger than ours, for $s = 6$ we get the same exponent as Danicic, and for $s \geqslant 7$ our exponent is better. That the constant $c_4(s)$ may not be replaced by a number greater than 2 is seen by taking the special quadratic form $\alpha(x_1^2+\ldots+x_s^2)$ where α is a number with bounded partial denominators in its continued fraction. However, it is conceivable that the theorem remains true with $c_4(s)$ replaced by 2 for $s > s_0$. For many special quadratic forms, $c_4(s)$ may be replaced by a number much larger than 2 (Schmidt [6]).

We will make use of Theorem 1 in order to prove Theorem 2. On the other hand, given an integral form $Q(x) = Q(x_1, \ldots, x_h)$ and applying Theorem 2 to $Q_1(x) = m^{-1}Q(x)$ and $N = m^{1/(c_4(h)-\varepsilon)}$, we note the existence of a solution of (1) with $0 < \max(|x_1|, \ldots, |x_h|) \leqslant N$, so that Theorem 1 holds with $e(h) = 1/(c_4(h)-\varepsilon)$, provided that m is large. Hence Theorem 1 may be regarded as a discrete version of Theorem 2.

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

2. Congruences

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

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

Suppose at first that q is odd. Then Q is equivalent to a form

$$y_1y_2+y_3y_4+\ldots+y_{h-2}y_{h-1}+ay_h^2,$$

and we may take S to be the subspace with $y_1 = y_3 = \ldots = y_{h-2} = y_h = 0$.

On the other hand, if q is even, the form may be seen to be equivalent to a form

$$c_1y_1^2+\ldots+c_hy_h^2+d_1y_1y_2+d_2y_2y_3+\ldots+d_{h-1}y_{h-1}y_h.$$

In this case we define S by $c_1^{q/2}y_1+\ldots+c_h^{q/2}y_h = 0$ and $y_2 = y_4 = \ldots$ $\ldots = y_{h-1} = 0$.

Proof of Theorem 1. If $m = u^2m_1$ and if $y_1, \ldots, y_h$ satisfy $Q(y_1, \ldots, y_h) \equiv 0 \pmod{m_1}$ and $0 < \max(|y_1|, \ldots, |y_h|) \leqslant m_1^{e(h)}$ then $x_1 = uy_1, \ldots, x_h = uy_h$ 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 h is odd by hypothesis, and put $d = (h-1)/2$.

For every prime p dividing m, there are by Lemma 1 integer points $\boldsymbol{v}_{p1}, \ldots, \boldsymbol{v}_{pd}$ which are linearly independent modulo p and such that $Q(\boldsymbol{x}) \equiv 0 \pmod{p}$ for each combination $\boldsymbol{x} = c_1\boldsymbol{v}_{p1}+\ldots+c_d\boldsymbol{v}_{pd}$ with integer coefficients. By the Chinese Remainder Theorem there are integer vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_d$ having $\boldsymbol{v}_i \equiv \boldsymbol{v}_{ip} \pmod{p}$ for each prime factor p of m. Write $\boldsymbol{v}_i = (v_{i1}, \ldots, v_{ih})$. We have $Q(\boldsymbol{x}) \equiv 0 \pmod{m}$ for

$$\boldsymbol{x} = c_1\boldsymbol{v}_1+\ldots+c_d\boldsymbol{v}_d+m\boldsymbol{z} \tag{6}$$

with integers $c_1, \ldots, c_d$ and with $\boldsymbol{z} = (z_1, \ldots, z_h)$ integral. According to Minkowski's Linear Forms Theorem, there are integers $c_1, \ldots, c_d, z_1, \ldots, z_h$, not all zero, with

$$\begin{gathered} |c_i| < m \quad (i = 1, \ldots, d), \\ |c_1v_{1j}+\ldots+c_dv_{dj}+mz_j| \leqslant m^{1-(d/h)} = m^{e(h)} \quad (j = 1, \ldots, h). \end{gathered} \tag{7}$$

The vector $\boldsymbol{x} = (x_1, \ldots, x_h)$ given by (6) satisfies (1) and $\max(|x_1|, \ldots, |x_h|) \leqslant m^{e(h)}$. If $c_1 = \ldots = c_d = 0$, then also $z_1 = \ldots = z_h = 0$, which is impossible. If, say, $c_1 \neq 0$, then by (7) there is a prime factor p of m with $c_1 \not\equiv 0 \pmod{p}$. In view of the linear independence of $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_d$ modulo p, we have $\boldsymbol{x} \not\equiv \boldsymbol{0} \pmod{p}$, whence $\boldsymbol{x} \neq \boldsymbol{0}$.

3. An Alternative Lemma. We now turn to Theorem 2. So let

$$Q(\boldsymbol{x}) = Q(x_1, \ldots, x_s) = \sum_{i,j} \lambda_{ij}x_ix_j$$

be a quadratic form with real coefficients. The matrix (λ_{ij}) may be supposed to be symmetric. We have

$$Q(\boldsymbol{x}) = x_1L_1(\boldsymbol{x})+\ldots+x_sL_s(\boldsymbol{x})$$

where $L_i(\boldsymbol{x}) = \lambda_{i1}x_1+\ldots+\lambda_{is}x_s$ $(i = 1, \ldots, s)$.

The symbol $\{\ldots\}$ will denote fractional parts: $\{x\} = x-[x]$.

LEMMA 2 (Alternative Lemma). *Let $\varepsilon > 0$, $s \geqslant 1$, $N \geqslant c_6(\varepsilon, s)$ and $N^{-c_4(s)+\varepsilon} \leqslant I < 1$. Then either*

(i) *for each interval* $\mathfrak{I}$ *of length* I *contained in* $0 \leqslant x < 1$, *there are integers* $n_1, \ldots, n_s$ *with* (4) *and with*

$$\{Q(n_1, \ldots, n_s)\} \in \mathfrak{I}$$

or

(ii) *there is a natural*

$$m \leqslant I^{-1} N^{s/4} \tag{8}$$

and for each h *in* $1 \leqslant h \leqslant (s+5)/3$ *there are* h *linearly independent integer vectors* $\boldsymbol{r}_\mu = (r_{1\mu}, \ldots, r_{s\mu})$ $(\mu = 1, \ldots, h)$ *with*

$$|r_{i\mu}| \leqslant I^{-(2/(s-h+1))} N^{s/4} \quad (1 \leqslant \mu \leqslant h,\ 1 \leqslant i \leqslant s) \tag{9}$$

and

$$\|m L_j(\boldsymbol{r}_\mu)\| < I^{-(2/(s-h+1))} N^{(s/4)-2} \quad (1 < \mu \leqslant h,\ 1 \leqslant j \leqslant s). \tag{10}$$

We proceed to deduce Theorem 2. Let $I = N^{-c_4(s)+\varepsilon}$. If the first alternative holds, then there are $n_1, \ldots, n_s$ with (4) and $0 \leqslant \{Q(n_1, \ldots \ldots, n_s)\} < N^{-c_4(s)+\varepsilon}$, and we are done. So we may assume the second alternative to hold. Pick h odd in $1 \leqslant h \leqslant (s+5)/3$ such that (3) is maximized.

Put

$$n_i = r_{i1} x_1 + \ldots + r_{ih} x_h \quad (1 \leqslant i \leqslant s)$$

with $x_1, \ldots, x_h$ yet to be determined. Write

$$\varphi_{\mu\nu} = m \sum_{j=1}^{s} \sum_{k=1}^{s} \lambda_{jk} r_{j\mu} r_{k\nu} = m \sum_{j=1}^{s} r_{j\mu} L_j(\boldsymbol{r}_\nu) \quad (1 \leqslant \mu, \nu \leqslant h).$$

We have

$$\|\varphi_{\mu\nu}\| = |\varphi_{\mu\nu} - b_{\mu\nu}| \quad (1 \leqslant \mu, \nu \leqslant h) \tag{11}$$

with certain integers $b_{\mu\nu}$ $(1 \leqslant \mu, \nu \leqslant h)$. By Theorem 1, there are integers $x_1, \ldots, x_h$, not all zero, with $|x_i| \leqslant m^{e(h)}$ $(i = 1, \ldots, h)$ and

$$\sum_{\mu=1}^{h} \sum_{\nu=1}^{h} b_{\mu\nu} x_\mu x_\nu \equiv 0 \pmod{m}. \tag{12}$$

Since the vectors $\boldsymbol{r}_1, \ldots, \boldsymbol{r}_h$ are linearly independent, we have $(n_1, \ldots, n_s) \neq (0, \ldots, 0)$, and from (8), (9) we get for sufficiently large N that

$$|n_i| \leqslant h m^{e(h)} \max_{1 \leqslant \mu \leqslant h} |r_{i\mu}| \leqslant I^{-e(h)-(2/(s-h+1))} N^{s/2}$$

$$\leqslant N^{(c_4(s)-\varepsilon)\left(\frac{1}{2}+\frac{1}{2h}+\frac{1}{s-h+1}\right)+\frac{s}{2}} \leqslant N \quad (1 \leqslant i \leqslant s).$$

On the other hand, by (11)

$$\|Q(n_1, \ldots, n_s)\| = \|Q(r_{11}x_1 + \ldots + r_{1h}x_h, \ldots, r_{s1}x_1 + \ldots + r_{sh}x_h)\|$$

$$= \left\| \frac{1}{m} \sum_{\mu=1}^{h} \sum_{\nu=1}^{h} \varphi_{\mu\nu} x_\mu x_\nu \right\|$$

$$\leqslant \left\| \frac{1}{m} \sum_{\mu=1}^{h} \sum_{\nu=1}^{h} b_{\mu\nu} x_\mu x_\nu \right\| + \frac{1}{m} \sum_{\mu=1}^{h} \sum_{\nu=1}^{h} |x_\mu| |x_\nu| \|\varphi_{\mu\nu}\|.$$

From (12), (9), (10) and since $|x_\mu| \leqslant m^{e(h)}$ $(1 \leqslant \mu \leqslant h)$, we get

$$\|Q(n_1, \ldots, n_s)\| \leqslant s^3 m^{2e(h)-1} \left(I^{-(2/(s-h+1))} N^{s/4}\right) \left(N^{-(2/(s-h+1))} N^{(s/4)-2}\right).$$

By virtue of (8) and of $2e(h) - 1 = 1/h$, this is

$$\leqslant s^3 I^{-(1/h)-(4/(s-h+1))} N^{(3s/4)-2},$$

and for large N it is

$$< N^{(c_4(s)-\varepsilon)((1/h)+(4/(s-h+1)))} N^{s-2} < N^{-c_4(s)+\varepsilon}.$$

4. Davenport's Lemma

LEMMA 3. *Let* $L_1, \ldots, L_s$ *be real linear forms in* $\boldsymbol{x} = (x_1, \ldots, x_s)$ *and with a symmetric coefficient matrix. Let* $N \geqslant 1$ *and let* $M_1, \ldots, M_s$ *be the first* s *successive minima of the convex body described by*

$$\left.\begin{aligned} |L_j(\boldsymbol{x}) - x_{s+j}| &< N^{-1} \\ |x_j| &< N \end{aligned}\right\} \quad (j = 1, \ldots, s)$$

with respect to the lattice of integer points in $2s$*-dimensional space. Then the number of integer points* $\boldsymbol{x} = (x_1, \ldots, x_s)$ *satisfying the simultaneous inequalities*

$$\left.\begin{aligned} \|L_j(\boldsymbol{x})\| &< N^{-1} \\ |x_j| &< N \end{aligned}\right\} \quad (j = 1, \ldots, s)$$

is $\ll (M_1 \cdot \ldots \cdot M_s)^{-1}$.

Here and in the sequel the constant implied by $\ll$ depends only on s or on s and ε.

This is Lemma 3 of Davenport [3]. Put

$$S(k) = \sum_{(n_1, \ldots, n_s) \in \mathfrak{N}} e\big(kQ(n_1, \ldots, n_s)\big),$$

where $e(x) = e^{2\pi i x}$, k is natural and $\mathfrak{N}$ is the set given by (4).

LEMMA 4 (Davenport's Alternative Lemma). *Suppose that* $1 \leqslant h \leqslant s$ *and*

$$Z \geqslant c_7(s) N^{(h-2)/h}. \tag{13}$$

Then either

(i) *the estimate*

$$|S(k)|^2 \leqslant c_8(s) Z^{s-h+1} N^{s+h-1} (\log N)^s$$

holds or

(ii) *there exist h linearly independent integer vectors $\boldsymbol{r}_\mu = (r_{1\mu}, \ldots, r_{s\mu})$ $(\mu = 1, \ldots, h)$ with*

$$\begin{matrix} \|2kL_j(\boldsymbol{r}_\mu)\| < Z^{-1}N^{-1} \\ |r_{j\mu}| < Z^{-1}N. \end{matrix} \qquad (1 \leqslant j \leqslant s,\ 1 \leqslant \mu \leqslant h)$$

This lemma was shown in the case $h = 5$ by Davenport [3]. The proof for general h follows along the same lines as that of Davenport.

Proof. Let $M_1, \ldots, M_s$ be the first s successive minima of the convex body described by

$$\begin{matrix} |2kL_j(\boldsymbol{x}) - x_{s+j}| < N^{-1} \\ |x_j| < N \end{matrix} \qquad (j = 1, \ldots, s) \tag{14}$$

with respect to the lattice $\boldsymbol{Z}^{2s}$, where $\boldsymbol{x} = (x_1, \ldots, x_s)$. Suppose at first that $M_h < Z^{-1}$. Then there exist h linearly independent integer points $\boldsymbol{R}_\mu = (r_{1\mu}, \ldots, r_{2s,\mu})$ $(\mu = 1, \ldots, h)$ with

$$\begin{matrix} |2kL_j(r_{1\mu}, \ldots, r_{s\mu}) - r_{s+j,\mu}| < Z^{-1}N^{-1} \\ |r_{j\mu}| < Z^{-1}N. \end{matrix} \qquad (1 \leqslant j \leqslant s,\ 1 \leqslant \mu \leqslant h) \tag{15}$$

We are going to show that the resulting s-dimensional vectors $\boldsymbol{r}_\mu = (r_{1\mu}, \ldots, r_{s\mu})$ $(\mu = 1, \ldots, h)$ are also linearly independent. Suppose this were not true. Then there would be integers $u_1, \ldots, u_h$ with

$$u_1 r_{i1} + \ldots + u_h r_{ih} = 0 \qquad (i = 1, \ldots, s) \tag{16}$$

and $(u_1, \ldots, u_h) \neq (0, \ldots, 0)$. By considering certain determinants of order $h-1$, and in view of (15), we may assume that

$$|u_i| \ll (Z^{-1}N)^{h-1} \qquad (i = 1, \ldots, h). \tag{17}$$

On the other hand (16) implies

$$u_1 L_j(\boldsymbol{r}_1) + \ldots + u_h L_j(\boldsymbol{r}_h) = 0 \qquad (j = 1, \ldots, s)$$

so that by (15) and (17)

$$|u_1 r_{s+j,1} + \ldots + u_h r_{s+j,h}| \ll Z^{-1}N^{-1}(Z^{-1}N)^{h-1} \qquad (j = 1, \ldots, s).$$

If the constant $c_7(s)$ in (13) is small enough this implies

$$u_1 r_{s+j,1} + \ldots + u_h r_{s+j,h} = 0 \qquad (j = 1, \ldots, s)$$

which contradicts the linear independence of $\boldsymbol{R}_1, \ldots, \boldsymbol{R}_h$. As a consequence, we obtain alternative (ii).

Now suppose that $M_h \geqslant Z^{-1}$. Let $\mathcal{N}$ be he number of integer solutions $(x_1, \ldots, x_s)$ of the simultaneous inequalities

$$\begin{matrix} \|2kL_j(x_1, \ldots, x_s)\| < N^{-1} \\ |x_j| < N \end{matrix} \qquad (j = 1, \ldots, s).$$

It is well known that

$$|S(k)|^2 \ll \mathcal{N} N^s (\log N)^s \tag{18}$$

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

$$\mathcal{N} \ll (M_1 \cdot \ldots \cdot M_s)^{-1}. \tag{19}$$

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

$$\mathcal{N} \ll N^{h-1} Z^{s-h+1}.$$

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 $\mathfrak{J}$ of length I, such that $\{Q(n_1, \ldots, n_s)\} \notin \mathfrak{J}$ for s-tuples $(n_1, \ldots, n_s)$ in the set $\mathfrak{N}$ given by (4). Choose $r > 1 + 10\varepsilon^{-1}s$. By a lemma of Vinogradov ([8], Lemma 12; or see [6], § 3), there is a function $\psi(x)$, periodic with period 1, having $\psi(x) = 0$ unless x lies in an integer translate of $\mathfrak{J}$, and having a Fourier expansion

$$\psi(x) = \tfrac{1}{2}I + \sum_{q \neq 0} c_q e(qx),$$

where

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

We have

$$\sum_{(n_1, \ldots, n_s) \in \mathfrak{N}} \psi\big(Q(n_1, \ldots, n_s)\big) = 0.$$

The Fourier expansion of ψ yields

$$\sum_{q \neq 0} |c_q|\,|S(q)| \ll N^s I. \tag{20}$$

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

$$\sum_{|q| \geqslant K} |c_q|\,|S(q)| \ll N^s \sum_{|q| \geqslant K} |c_q| \ll N^s I \sum_{q=K}^{\infty} (qI)^{-r}$$
$$\ll N^s (IK)^{1-r} \ll N^{s-(\varepsilon/10)(r-1)} \ll 1 = o(N^s I),$$

by our choice of r. Thus from (20), and since $|c_q| \leqslant I$ and $|S(-q)| = |S(q)|$, we have

$$\sum_{q=1}^{K} |S(q)| \gg N^s.$$

Hence there is a q_0, $1 \leqslant q_0 \leqslant K \leqslant I^{-1}N^{s/10}$ with

$$|S(q_0)|^2 \gg N^{2s}K^{-2}. \tag{21}$$

Now let h be odd with $1 \leqslant h \leqslant (s+5)/3$. Then by the lower bound for I in the hypothesis of Lemma 2, the inequality (13) holds for

$$Z = N^{1-(s/(4(s-h+1)))}I^{2/(s-h+1)}.$$

With this choice of Z we have

$$Z^{s-h+1}N^{s+h-1}(\log N)^s \leqslant N^{2s-(s/4)}I^2N^{s/20} = N^{2s-(s/5)}I^2 \leqslant N^{2s}K^{-2},$$

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

[1] R. J. Cook, *On the fractional parts of an additive form*, Proc. Cambridge. Phil. Soc. 72 (1972), pp. 209–212.
[2] I. Danicic, *An extension of a theorem of Heilbronn*, Mathematika 5 (1958), pp. 30–37.
[3] H. Davenport, *Indefinite quadratic forms in many variables (II)*, Proc. London Math. Soc. (3) 8 (1958), pp. 109–126.
[4] H. Heilbronn, *On the distribution of the sequence θn^2 (mod 1)*, Quart. J. Math. 19 (1948), pp. 249–256.
[5] H. P. Schlickewei, *On indefinite diagonal forms in many variables* (to appear).
[6] W. M. Schmidt, *Small fractional parts of polynomials*, A. M. S. Regional Conference Series in Math. (to appear).
[7] B. Segre, *Teoria di Galois, fibrazioni proiettive e geometrie non desarguesiane*, Ann. Mat. Pura Appl. (4) 64 (1964), pp. 1–76.
[8] I. M. Vinogradov, *The method of trigonometric sums in the theory of numbers* (English transl.), Wiley-Interscience, 1954.

POLISH ACADEMY OF SCIENCES, Warsaw
UNIVERSITY OF COLORADO AND MATH. INST. UNIV. FREIBURG
UNIVERSITY OF COLORADO, Boulder

Received on 21. 10. 1977 (992)

ACTA ARITHMETICA
XXXVII (1980)

On the differences of additive functions, II

by

P.D.T.A. Elliott* (Boulder, Colo.)

In memory of Professor P. Turán

An arithmetic function $f(n)$ is said to be additive if it satisfies the relation $f(ab) = f(a)+f(b)$ whenever a and b are coprime (positive) integers. Concerning real-valued additive functions we have:

THEOREM 1. *Let a be a positive integer. Then the following three conditions are equivalent:*

(i) *There is a constant B so that the inequality*

$$\sum_{n\leqslant x} |f(n+a)-f(n)|^2 \leqslant Bx$$

holds for all $x \geqslant 2$;

(ii) *There is a constant C so that the inequality*

$$\sum_{n\leqslant x} n^{-1}|f(n+a)-f(n)|^2 \leqslant C\log x$$

holds for all $x \geqslant 2$;

(iii) *There is a constant A so that the series*

$$\sum_{p} \sum_{k=1}^{\infty} p^{-k}|f(p^k)-A\log p^k|^2$$

converges.

As a companion to this result we have

THEOREM 2. *Let λ and μ be real numbers, $\lambda+\mu \neq 0$. Let a and b be integers. Then the following three conditions are equivalent:*

(i) *There is a constant B so that the inequality*

$$\sum_{n\leqslant x} |\lambda f(n+a)+\mu f(n+b)|^2 \leqslant Bx$$

holds for all $x \geqslant 2$;

* Supported by N. S. F. contract number MCS 75-08233.