ACTA ARITHMETICA
XXXVII (1980)

On the equation $1^k+2^k+\ldots+x^k=y^z$

by

K. Győry (Debrecen), R. Tijdeman (Leiden) and M. Voorhoeve
(Amsterdam)

In respectful memory of Professor P. Turán

1. Introduction. In 1956 J. J. Schäffer [4] proved that for fixed k and $z>1$ the title equation has an infinite number of solutions in positive integers x, y only in the following cases: (I) $k=1$, $z=2$, (II) $k=3$, $z\in\{2,4\}$, (III) $k=5$, $z=2$. In all other cases the number of solutions was shown to be bounded by a constant depending only on k. He conjectured that the only other solutions have $x=y=1$, apart from $k=z=2$, $x=24$, $y=70$. Schäffer's complicated proof used an ineffective method due to Thue and Siegel. On applying the Gel'fond–Baker method, we are able to prove the following generalization.

Theorem 1. *Let $p_1,\ldots,p_t$ be a finite set of fixed primes and denote by S the set of integers composed of these primes. Let r and $k\geqslant 2$ be fixed rational integers with $k\notin\{3,5\}$ if $r=0$. Then the equation*

$$r+1^k+2^k+\ldots+x^k=wy^z \tag{1}$$

in positive integers $w\in S$, x, $y>1$, $z>1$ has only finitely many solutions.

By the effectiveness of the used method, upper bounds for w, x, y and z can be determined effectively. Note that it is a consequence of Theorem 1 that for any integers $a>1$, b and $k\geqslant 2$ the equation

$$a^k+(a+1)^k+\ldots+x^k=by^z$$

has only finitely many solutions in integers $x>a$, $y>1$ and $z>1$.

The deduction of Theorem 1 from recent results on Diophantine equations is straightforward if the polynomial $r+1^k+2^k+\ldots+x^k$ in x is known to have at least three simple zeros. This polynomial is closely related to the Bernoulli polynomial $B_{k+1}(x)$, namely

$$1^k+2^k+\ldots+x^k=\frac{1}{k+1}\{B_{k+1}(x+1)-B_{k+1}\}, \tag{2}$$

where $B_{k+1} = B_{k+1}(0)$ is the $(k+1)$-th Bernoulli number. We prove slightly more than we need.

THEOREM 2. *For every $r \in \mathbf{Z}$ the polynomial*

$$P(x) = B_q(x) - B_q + r$$

has at least three simple zeros if $q = 3$ and at least four simple zeros if $q \geqslant 4$, unless $r = 0$ and $q \in \{4, 6\}$.

In case q is odd, a straightforward generalization of an argument of Brillhart [2] shows that all zeros of $P(x)$ are simple. The case q is even is more complicated.

In Section 2 we quote the results on Bernoulli polynomials which we need for the proof of Theorem 2. In Sections 3, 4 and 5 the proof is given in case q is odd, $q \equiv 0 \pmod 4$ and $q \equiv 2 \pmod 4$ respectively. In Section 6 we quote the results on Diophantine equations which we use in the deduction of Theorem 1. The proof itself is given in Section 7. Some remarks on generalizations and related results are made in Section 8.

We note that all proofs of results in this paper are effective and we make no further reference to this aspect of the method.

2. For $q = 0, 1, 2, \ldots$, the Bernoulli polynomials $B_q(x)$ are defined by

$$\frac{ze^{xz}}{e^z - 1} = \sum_{q=0}^{\infty} \frac{B_q(x) z^q}{q!}, \qquad |z| < 2\pi.$$

Their expansion around the origin is given by

$$B_q(x) = \sum_{s=0}^{q} \binom{q}{s} B_s x^{q-s},$$

where $B_0 = 1$, $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}, \ldots$ are the Bernoulli numbers. One has $B_{2k+1} = 0$ for $k = 1, 2, 3, \ldots$ For the following well-known properties of Bernoulli polynomials and numbers we refer to Rademacher [3], pp. 1–17.

(3) $$B_q(1-x) = (-1)^q B_q(x).$$

(4) $$B_q(x+1) = B_q(x) + qx^{q-1}.$$

So $B_q(2) = B_q(1) + q = B_q + q$ for $q \geqslant 2$. By induction, one finds (2).

(5) $$B_q'(x) = qB_{q-1}(x).$$

(6) $$(-1)^{k-1} B_{2k} > 0 \quad \text{for} \quad k \geqslant 1.$$

(7) (The von Staudt–Clausen Theorem) The denominator of the Bernoulli number B_{2k} is the product of those different primes p for which $p-1$ divides $2k$.

More precisely,

$$B_{2k} = G_{2k} - \sum_{(p-1)|2k} \frac{1}{p},$$

where G_{2k} is an integer.

(8) $$|B_{2k}| > 2\cdot(2k)!/(2\pi)^{2k}.$$

(9) $$B_q(\tfrac{1}{2}) = (2^{1-q} - 1)B_q.$$

(10) The polynomials $B_{2k+1}(x)$ have no zeros in the segment $(\frac{1}{2}, 1)$. Hence by (5) the polynomials $B_{2k}(x)$ are monotonic in $(\frac{1}{2}, 1)$. In view of (3), (6) and (9) the polynomials $B_{2k}(x)$ are monotonically increasing in $(\frac{1}{2}, 1)$ if k is odd, decreasing if k is even.

Proof of Theorem 2. We distinguish several cases.

3. Suppose q is odd. Choose $d \in \mathbf{N}$ such that $dP(x)$ is a primitive polynomial in $\mathbf{Z}[x]$, that is a polynomial with integer coefficients having no common factor. By (7), d is even and squarefree, whereas for $l = 1, 2, 4, 6, \ldots, q-1$,

$$\binom{q}{l} dB_l \equiv \binom{q}{l} \pmod 2.$$

Now

$$dP(x) = dx^q + \sum_{l=1}^{q-1} dB_l \binom{q}{l} x^{q-l} + dr \equiv x^{q-1} + \sum_{\lambda=1}^{\frac{1}{2}(q-1)} \binom{q}{2\lambda} x^{q-2\lambda} \pmod 2.$$

Hence,

$$d\big(P(x) + xP'(x)\big) \equiv qx^{q-1} + \sum_{\lambda=1}^{\frac{1}{2}(q-1)} \binom{q}{2\lambda}(1+q-2\lambda)x^{q-2\lambda} \equiv x^{q-1} \pmod 2.$$

Any common factor of $dP(x)$ and $dP'(x)$ must therefore be congruent to a power of $x \pmod 2$. Since $dP'(0) = qdB_{q-1} \equiv 1 \pmod 2$ we find that $dP(x)$ and $dP'(x)$ are relatively prime (mod 2). So any irreducible common divisor of $dP(x)$ and $dP'(x)$ in $\mathbf{Z}[x]$ must be of the shape $2R(x)+1$. Then $dP(x)$ is divisible by $(2R(x)+1)^2$ and the leading coefficient d of $dP(x)$ is divisible by the leading coefficient of $(2R(x)+1)^2$. Since $4 \nmid d$, this is impossible unless R is a constant. All the zeros of $P(x)$ are therefore simple. A special noteworthy case occurs when $r = 0$, so $P(x) = B_q(x)$.

4. Suppose q is even. The derivative $P'(x) = qB_{q-1}(x)$ of P has only simple zeros, so each zero of $P(x)$ is of multiplicity less than 3. Choose $d \in \mathbf{N}$ such that $dP(x)$ is a primitive polynomial in $\mathbf{Z}[x]$. Let $T(x)$ be the g.c.d. of $dP(x)$ and $dP'(x)$. Then $T(x) \in \mathbf{Z}[x]$ is primitive and

$$dP(x) = T^2(x)Q(x),$$

where $Q(x) \in \mathbf{Z}[x]$ contains all the simple zeros of $P(x)$. The theorem is equivalent to the statement that $\deg Q \geqslant 4$ unless $q \in \{4, 6\}$ and $r = 0$. By (7), d is squarefree. Since $P(x)$ is monic, we find that $T(x)$ must also be monic. Since $r \in \mathbf{Z}$, either $2^q dP(\frac{1}{2})$ or $2^{q-1}dP(\frac{1}{2})$ is an odd integer, so $P(\frac{1}{2}) \neq 0$. By (3), $P(1-x) = P(x)$. So for each zero ξ of $P(x)$ there is a zero $1-\xi$ of the same multiplicity. Therefore $T(x)$ is of even degree and $\deg Q \equiv q \pmod 4$.

Now suppose that $q \equiv 0 \pmod 4$ and assume that $\deg Q < 4$, so $\deg Q = 0$. Hence, since $dP(x)$ is primitive, $Q(x) = \pm 1$. Thus $d = 1$. The denominator of B_{2k} is divisible by 6 for $k = 1, 2, 3, \ldots$ So necessarily $6 \mid \binom{q}{2k}$ for $k = 1, 2, \ldots, \frac{1}{2}q-1$. Write $q = t2^\lambda$, where t is odd. Then $2 \nmid \binom{q}{2k}$, which gives a contradiction unless $t = 1$. So $q = 2^\lambda$. Next choose $\mu \in N$ such that $3^\mu < q \leqslant 3^{\mu+1}$ and write $q = 3^\mu + s3^\nu$, where $3 \nmid s$. Since q is even, s must be odd. Then $3 \nmid \binom{q}{(s-1)3^\nu}$, which gives a contradiction unless $s = 1$.

So $q = 2^\lambda = 3^\mu + 3^\nu$. Since any power of 3 is congruent to 1 or 3 (mod 8), the only solutions of this equation are $q = 2$ or $q = 4$. So $q = 4$. Since $P'(x) = 4B_3(x)$ has the only roots 0, $\frac{1}{2}$ and 1 and since $P(\frac{1}{2}) \neq 0$, we must have $P(0) = P(1) = 0$, so $r = 0$. The theorem is thus proved in this case.

5. Suppose that $q \equiv 2 \pmod 4$ and assume that $\deg Q < 4$. Then $\deg Q = 2$. Moreover, since $q > 2$, we find that d is even. By (3), $Q(x) = Q(1-x)$. Furthermore, $T(x)$ is monic. Hence, for some $c \in \mathbf{Z}$,

$$dP(x) = (dx^2 - dx + c)T^2(x). \tag{11}$$

Since $dP(x)$ is primitive, $(d, c) = 1$. It follows from

$$(dx^2 - dx + c) \mid \left(dx^q - \tfrac{1}{2}dqx^{q-1} + \tfrac{1}{6}d\binom{q}{2}x^{q-2} + \ldots\right)$$

that

$$(dx^2 - dx + c) \mid \left(-\tfrac{1}{2}d(q-2)x^{q-1} + \left(\tfrac{1}{6}d\binom{q}{2} - c\right)x^{q-2} + \ldots\right)$$

and therefore $d \mid \left(\frac{1}{6}d\binom{q}{2} - c\right)$. Hence, $\left(d, \frac{1}{6}d\binom{q}{2}\right) = 1$. Thus $d \mid 6$. Suppose that $d = 6$. Then $3 \nmid c$ and $3 \nmid q$. By (11), (3) and (4) we have

$$6P(1) = cT(1)^2 = 6r,$$

$$6P(2) = (12 + c)T^2(2) = 6r + 6q.$$

So both $6r$ and $6(r+q)$ are divisible by 3^2. By $3 \nmid q$ this is impossible. So we find that $d = 2$.

Suppose that $p \mid c$ for some odd prime p. For $S(x) \in \mathbf{Z}[x]$ we denote by $\big(S(x)\big)_p$ the image of S in $\mathbf{Z}_p[x]$ under the canonical mapping. Choose

$T_1(x)$ such that

$$\big(T(x)\big)_p = \big(x^k \cdot T_1(x)\big)_p,$$

where $(x)_p \nmid \big(T_1(x)\big)_p$, so $p \nmid T_1(0)$. Then

$$\big(2P(x)\big)_p = \big((2x^2 - 2x)(x^{2k} \cdot T_1^2(x))\big)_p.$$

By comparing the coefficients of x^{2k+1} we find

$$0 \not\equiv -2T_1^2(0) \equiv 2\binom{q}{2k+1}B_{q-2k-1} \pmod p.$$

Consequently $B_{q-2k-1} = B_1$, so $q = 2k+2$. Thus $\big(T_1(x)\big)_p$ is constant. Since $T(x)$ is monic, $\big(T^2(x)\big)_p = (x^{2k})_p = (x^{q-2})_p$. Hence, by (11),

$$(2x^q - 2x^{q-1})_p = \left(2x^q - qx^{q-1} + \tfrac{1}{3}\binom{q}{2}x^{q-2} + \ldots\right)_p.$$

So $q \equiv 2 \pmod p$ and $\frac{1}{3}\binom{q}{2} \equiv 0 \pmod p$. This is impossible, so $c = \pm 1$. We therefore have either $(2x^2 - 2x + 1) \mid 2P(x)$ and $r = B_q(0) - B_q(\frac{1}{2} + \frac{1}{2}i)$ or $(2x^2 - 2x - 1) \mid 2P(x)$ and $r = B_q(0) - B_q(\frac{1}{2} + \frac{1}{2}\sqrt{3})$. We investigate these cases separately.

Suppose that $P(x) = B_q(x) - B_q(\frac{1}{2} + \frac{1}{2}i)$. Put $\sigma = \frac{1}{4}(q-2)$. Since $r \in \mathbf{Z}$ is real and $(\frac{1}{2} + \frac{1}{2}i)^2 = \frac{1}{2}i$, we have

$$\begin{aligned} -r &= B_q(\tfrac{1}{2} + \tfrac{1}{2}i) - B_q(0) = \operatorname{Re}\left\{\sum_{k=0}^{q-2}\binom{q}{k}(\tfrac{1}{2} + \tfrac{1}{2}i)^{q-k}B_k\right\} \\ &= 0 + \operatorname{Re}\{-\tfrac{1}{2}q(\tfrac{1}{2} + \tfrac{1}{2}i)^{q-1}\} + \tfrac{1}{6}\binom{q}{2}(\tfrac{1}{2} + \tfrac{1}{2}i)^{q-2} + 0 + B_6\binom{q}{6}(\tfrac{1}{2} + \tfrac{1}{2}i)^{q-6} + \ldots \\ &= \left(-\tfrac{1}{4}q + \tfrac{1}{6}\binom{q}{2}\right)(-\tfrac{1}{4})^\sigma + B_6\binom{q}{6}(-\tfrac{1}{4})^{\sigma-1} + B_{10}\binom{q}{10}(-\tfrac{1}{4})^{\sigma-2} + \ldots \end{aligned}$$

Since $d = 2$, $2B_k\binom{q}{k} \in \mathbf{Z}$ for $k = 2, \ldots, q-2$. Hence, $4^\sigma B_6\binom{q}{6}(-\frac{1}{4})^{\sigma-1} = \pm 4B_6\binom{q}{6}$ is an even integer. Similarly $4^\sigma B_{4k+2}\binom{q}{4k+2}(-\frac{1}{4})^{\sigma-k}$ are even integers for $k = 2, 3, \ldots$ It follows that

$$4^\sigma\left(-\tfrac{1}{4}q + \tfrac{1}{6}\binom{q}{2}\right)(-\tfrac{1}{4})^\sigma = (-1)^\sigma\tfrac{1}{12}q(q-4)$$

is an integer, which is apparently odd. Consequently $4^\sigma r$ is an odd integer, showing by $\sigma \geqslant 1$ that $r \notin \mathbf{Z}$. This is a contradiction.

Suppose that $P(x) = B_q(x) - B_q(\frac{1}{2} + \frac{1}{2}\sqrt{3})$. One finds that

$$B_6(x) = x^6 - 3x^5 + \tfrac{5}{2}x^4 - \tfrac{1}{2}x^2 + B_6.$$

So

$$B_6(x) - B_6(0) = \tfrac{1}{2}(2x^2 - 2x - 1)(x^2 - x)^2.$$

Thus $r = B_6(0)-B_6(\frac{1}{2}+\frac{1}{2}\sqrt{3}) = 0$ if $q = 6$, which agrees with our theorem. So let $q > 6$, whence $q \geqslant 10$. By (6), $B_q(1)$ is positive and, by (9), $B_q(\frac{1}{2})$ is negative. Finally, by (10), $B_q(x)$ is monotonically increasing in $(\frac{1}{2}, 1)$. We have by (4) and (3)

$$B_q(\tfrac{1}{2}+\tfrac{1}{2}\sqrt{3}) = B_q(-\tfrac{1}{2}+\tfrac{1}{2}\sqrt{3})+q(-\tfrac{1}{2}+\tfrac{1}{2}\sqrt{3})^{q-1} > B_q(-\tfrac{1}{2}+\tfrac{1}{2}\sqrt{3})$$
$$= B_q(1\tfrac{1}{2}-\tfrac{1}{2}\sqrt{3}) > B_q(\tfrac{1}{2}).$$

Suppose that $B_q(\frac{1}{2}+\frac{1}{2}\sqrt{3}) < B_q(1)$. Then there is a $\varrho \in (\frac{1}{2}, 1)$ such that $B_q(\varrho) = B_q(\frac{1}{2}+\frac{1}{2}\sqrt{3})$. Hence $P(x)$ has a simple zero in $(\frac{1}{2}, 1)$, which gives a contradiction. So $B_q(\frac{1}{2}+\frac{1}{2}\sqrt{3}) \geqslant B_q(1) > 0$. Since $B_q'(1) = 0$ and $B_q''(1) < 0$ there is an $\varepsilon > 0$ such that $B_q(1+\varepsilon) < B_q(1) \leqslant B_q(\frac{1}{2}+\frac{1}{2}\sqrt{3})$. Since $q \geqslant 10$ we have by (4), (9) and (8)

$$B_q(1\tfrac{1}{2}) = B_q(\tfrac{1}{2})+q(\tfrac{1}{2})^{q-1} \leqslant (2^{-9}-1)\frac{10!}{(2\pi)^{10}}+10\cdot 2^{-9} < 0 < B_q(\tfrac{1}{2}+\tfrac{1}{2}\sqrt{3}).$$

Let σ be the maximum of $B_q(x)$ in the interval $[1+\varepsilon, 1\frac{1}{2}]$ and let this maximum be assumed at the point $\tau \in (1+\varepsilon, 1\frac{1}{2})$. Since $\frac{1}{2}+\frac{1}{2}\sqrt{3}$ was a simple zero of $P(x)$, we have that $B_q(\frac{1}{2}+\frac{1}{2}\sqrt{3}) < \sigma$. Thus $P(x)$ changes sign in $(1, \tau)$ and in $(\tau, 1\frac{1}{2})$, so $P(x)$ must have at least two zeros of odd multiplicities in $(1, 1\frac{1}{2})$, which by (3) implies that $\deg Q \geqslant 4$. This final contradiction proves Theorem 2.

6. For the proof of Theorem 1 we need the following results.

LEMMA 1. *Let S be the set of all non-zero integers composed of primes from some fixed finite set. Let $P \in \mathbf{Q}[x]$ be a polynomial with at least two distinct zeros. Then the equation*

$$P(x) = wy^z$$

in integers $w \in S$, $x, y > 1$, z implies that $z < C$, where C is a constant depending only on P and S.

Proof. This is a direct consequence of [5], Theorem 2.

LEMMA 2. *Let $P \in \mathbf{Q}[x]$ be a polynomial with at least three simple zeros. Let b and m be fixed integers with $b \neq 0$ and $m \geqslant 2$. Then the equation*

$$P(x) = by^m$$

has only finitely many solutions in integers x and y.

Proof. This follows easily from a result of Baker [1] giving the stated result in case $P(x) \in \mathbf{Z}[x]$, $b = 1$. Let d be an integer such that $dP(x) \in \mathbf{Z}[x]$. Then $b^{m-1}d^mP(x)$ is a polynomial with integer coefficients satisfying

$$b^{m-1}d^mP(x) = (bdy)^m.$$

According to Baker's result there are only finitely many integer solutions x and bdy. This proves our assertion.

7. Proof of Theorem 1. We know from Theorem 2 that the polynomial

$$r+1^k+2^k+\dots+x^k = \frac{1}{k+1}\{B_{k+1}(x+1)-B_{k+1}+r(k+1)\} \tag{12}$$

has at least two distinct zeros. Hence it follows from equation (1) by applying Lemma 1 that z is bounded. We therefore may assume that z is fixed. We can incorporate any zth power in y^z. Doing so there are only z^t possibilities for w. Hence we may assume without loss of generality that w is fixed. So we have obtained an equation

$$r+1^k+2^k+\dots+x^k = by^m, \quad b \neq 0,\ m \geqslant 2,$$

in integers x and y. According to Theorem 2 the polynomial on the right side of (12) has at least three simple zeros, unless $r = 0$ and $k \in \{3, 5\}$. On applying Lemma 2 we find that there are only finitely many solutions x, y. Thus the number of solutions (w, x, y, z) of (1) is finite, unless $r = 0$ and $k \in \{3, 5\}$.

8. Remark 1. R. J. Stroeker proved that the Diophantine equation

$$q = 3^\mu+3^\nu = 5^\sigma+5^\tau$$

has the only solutions $q = 2, 6, 10$ or 30. It follows from this result that, under the assumptions in Section 5, $d = 2$ if and only if $q = 6, 10$ or 30. This gives an alternative for the last part of the proof of Theorem 2. A similar idea was used in the proof of Schäffer's result mentioned in the introduction.

Remark 2. The proof of Theorem 2 remains valid if we replace r by r/s, where s is a squarefree odd integer. This implies that Theorem 1 also holds if (1) is replaced by the equation

$$r+s(1^k+2^k+\dots+x^k) = wy^z$$

for some squarefree odd integer s.

Remark 3. It is possible that the condition in Theorem 1 that k is fixed is unnecessary. However, we are not even able to prove that for fixed r and $n \geqslant 2$ the equation

$$r+1^x+2^x+\dots+n^x = wy^z$$

has only finitely many solutions in positive integers $w \in S$, x, $y > 1$, $z > 1$. Using the fact that the term n^x dominates the left side if x is large, one can deduce that z is bounded and that the greatest prime factor of y tends to infinity as $x \to \infty$. For the first fact one can apply [6], Theorem 1 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 a, there exists a natural $n \leqslant N$ with*

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

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 a_1, a_2, there exist integers n_1, n_2 not both zero, having $|n_1|, |n_2| \leqslant N$ and*

$$\|a_1 n_1^2 + a_2 n_2^2\| < N^{-1+\varepsilon}.$$

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