# ON THE NUMBER OF SOLUTIONS OF $m=\sum_{i=1}^{k} x_i^k$

P. ERDÖS AND E. SZEMEREDI

Denote by $r_{k,l}(n)$ the number of solutions of

$$n=\sum_{i=1}^{l} x_i^k$$

in positive integers $x_i$. The well-known hypothesis $K$ of Hardy and Littlewood states that for every $\varepsilon>0$,

$$r_{k,k}(n)=O(n^{\varepsilon}). \tag{1}$$

(1) is well-known for $k=2$, in fact for $n>n_0(\varepsilon)$,

$$r_{2,2}(n)<n^{(1+\varepsilon)\log 2/\log\log n}, \tag{2}$$

and (2) does not hold for every $n$ if $\log 2$ is replaced by a smaller constant. Nearly 40 years ago Mahler [7] disproved the hypothesis for $k=3$. He showed in fact that for infinitely many $n$ ($c_1, c_2, \ldots$ denote positive absolute constants),

$$r_{3,3}(n)>c_1 n^{1/12}. \tag{3}$$

It is possible that, for all $n$,

$$r_{3,3}(n)<c_2 n^{1/12}, \tag{4}$$

but nothing is known about this. It is probable that the $K$-hypothesis fails for every $k>3$ too, but probably

*AMS* 1970 *subject classifications*. Primary 10B15, 10J99.

$$\sum_{n=1}^{x} (r_{k,k}(n))^2 < x^{1+\varepsilon} \tag{5}$$

for every $\varepsilon$ if $x > x_0(\varepsilon)$. (5) would be just as useful for Waring's problem as the $K$-hypothesis.

Chowla [1] proved that for $k \geqq 5$, $r_{k,k}(n) \neq O(1)$, and Chowla and Erdös [3] proved that, for every $k \geqq 2$ and infinitely many $n$,

$$r_{k,k}(n) > \exp(c_k \log n / \log\log n).$$

Mordell proved that $r_{3,2}(n) \neq O(1)$, and Mahler [8] proved that, for infinitely many $n$, $r_{3,2}(n) > (\log n)^{1/4}$. As far as we know there is no nontrivial upper bound for $r_{3,2}(n)$ and almost nothing is known about $r_{k,l}(n)$ for $l < k$, $k > 3$.

Another very difficult problem is to estimate $A_{k,l}(x)$, the number of integers $m \leqq x$ for which

$$m = \sum_{i=1}^{l} x_i^k$$

is solvable. A classical result of Landau states that

$$A_{2,2}(x) = (C + o(1))\, x/(\log x)^{1/2}.$$

Mahler and Erdös [4] proved that, for every $k > 2$, $A_{k,2}(x) > \alpha_k x^{2/k}$ ($\alpha_k > 0$), and Hooley proved $A_{k,2}(x) = (c_k + o(1))\, x^{2/k}$. It seems certain that, for every $l < k$,

$$A_{k,l} > \alpha_{k,l} x^{l/k} \quad \text{and} \quad A_{k,k}(x) > x^{1-\varepsilon}$$

for every $\varepsilon > 0$, if $x > x_0(\varepsilon)$. Unfortunately we have no contribution towards settling these classical problems; for important partial results see the papers of Davenport [2].

P. Erdös [5] proved the following result.

Let $r_1 < \cdots < r_k < n$, $k > n^{1 - c_1/\log\log n}$, $c_1 < \frac{1}{2}\log 2$. Then for $n > n_0(c_1)$, there is an $m$ so that the number of solutions of $m = r_i^2 - r_j^2$ is greater than

$$\exp(c_2 \log n / \log\log n).$$

He also proved that for infinitely many $n$ the number of solutions of $n = p^2 + q^2$, $p$, $q$ primes, is greater than $\exp(c_3 \log n/\log\log n)$. P. Erdös states without giving the proof that for every $k$ there is an $n_k$ so that the number of solutions of $n_k = p^3 + q^3 + r^3$ is greater than $k$. The analogous result seems to be unknown for more than three summands.

In the present note we prove the following:

THEOREM. *Let $t$ be a positive integer, $c_1$ a positive number, and $l$ and $n$ positive integers satisfying $l>c_1 n$. Let $a_1<\cdots<a_l$ be positive integers smaller than $n$ but otherwise arbitrary. If $n>n_0(c_1, t)$ there exists an integer $m$ such that the equation*

$$m=\sum_{j=1}^{k} a_{i_j}^k, \qquad 1\leqq i_1<\cdots<i_k\leqq l,$$

*has more than $t$ solutions.*

Before we prove our theorem we wish to state a few well-known and very difficult problems in additive number theory.

Denote by $f_k(n)$ the largest set of integers $1\leqq a_1<\cdots<a_l\leqq n$ for which all the sums

$$\sum_{i=1}^{l} \varepsilon_i a_i, \qquad \varepsilon_i=0 \text{ or } 1, \qquad \sum_{i=1}^{l} \varepsilon_i\leqq k$$

are all distinct. Erdös and Turán conjectured

$$f_2(n)=n^{1/2}+O(1). \tag{6}$$

This problem seems very deep. Erdös, Turán and Lindström [6] proved

$$f_2(n)\leqq n^{1/2}+n^{1/4}+1$$

and recently Szemeredi proved $f_2(n)<n^{1/2}+o(n^{1/4})$; the proof is very complicated. The results of Singer [9] immediately imply $f_2(n)\geqq(1+o(1))\, n^{1/2}$. P. Erdös often offered 300 dollars for a proof or disproof of the conjecture (6).

Chowla and Ryser conjectured that

$$f_k(n)=(1+o(1))\, n^{1/k}. \tag{7}$$

They proved $f_k(n)\geqq(1+o(1))\, n^{1/k}$. P. Erdös offers 100 dollars for a proof or disproof of (7). The methods used for $f_2(n)$ seem to break down completely.

Finally denote by $F(n)$ the largest set of integers $1\leqq a_1<\cdots<a_l<n$ for which all the sums $\sum_{i=1}^{l} \varepsilon_i a_i$, $\varepsilon_i=0$ or 1 are all distinct. P. Erdös and L. Moser proved

$$F(n)\leqq\frac{\log n}{\log 2}+\frac{\log\log n}{2\log 2}+c,$$

and Conway and Guy showed that for $t>22$, $F(2^t)\geqq t+2$. P. Erdös asked 40 years

ago: Is it true that

$$(*) \qquad F(n)=\log n/\log 2+O(1)?$$

Erdös offers 300 dollars for a proof or disproof of (8).

We now prove our theorem. The proof is rather complicated and to motivate it we first try to explain its plan which follows [3].

Let $s$ be sufficiently large but fixed, $A$ will denote the sequence $1\leqq a_1<\cdots<a_l\leqq n$, $l>c_1 n$. $A(u, d, n)$ denotes the number of integers of the sequence $A$ satisfying

$$a_i\equiv u \pmod d.$$

Suppose that we have found a square-free integer $T_r$, $r>r_0(k, s, t, c)$, all of whose prime factors $p_1,\ldots, p_r$ are sufficiently large so that for every $j$, $1\leqq j\leqq r$,

$$(8) \qquad A(0, T_r/p_j; n)>lp_j/2T_r;$$

and the number of residue classes $u \pmod{T_r p_j^{k-1}}$, $u\equiv 0 \pmod{T_r/p_j}$ (the number of these residue classes is $p_j^k$) which do not satisfy

$$(9) \qquad A(u, T_r p_j^{k-1}; n)>l/sT_r p_j^{k-1}$$

is less than $p_j^k/8k$ for $j=1,\ldots, r$. Then we can prove our theorem by the method of [3].

To see this denote by $F(T_r)$ the number of solutions of the congruence (in distinct $a$'s)

$$(10) \qquad \sum_{i=1}^{k} a_i^k\equiv 0 \pmod{T_r^k} \qquad (1\leqq i\leqq l),$$

and let $F_j(T_r)$ denote the number of those solutions of (10) for which

$$a_i\equiv 0 \pmod{T_r/p_j}, \qquad a_i\not\equiv 0 \pmod{p_j}, \qquad i=1, 2,\ldots, k.$$

Clearly

$$(11) \qquad \sum_{j=1}^{r} F_j(T_r)\leqq F(T_r).$$

Next we estimate $F_j(T_r)$ from below. The first $k-2$ summands of (10) we choose arbitrarily subject only to

$$(12) \qquad a_i\equiv 0 \pmod{T_r/p_j}, \qquad a_i\not\equiv 0 \pmod{p_j}.$$

The number of choices of $a_i$ satisfying (12) is, by (8), greater than

$$(13) \qquad lp_j/2T_r-n/T_r>lp_j/4T_r$$

by $l>c_1 n$, if the prime factors of $T_r$ are greater than, say, $10/c_1$. From (13) we obtain that the number of choices of $k-2$ distinct $a$'s satisfying (12) is greater than

$$\left(\frac{lp_j}{10T_r}\right)^{k-2} \Big/ (k-2)! > \frac{1}{(10k)^k}\left(\frac{lp_j}{T_r}\right)^{k-2}. \tag{14}$$

We have to choose $a_{k-1}$ and $a_k$ so that besides satisfying (12) they should satisfy

$$a_{k-1}^k + a_k^k \equiv -\sum_{i=1}^{k-2} a_i^k \pmod{p_j^k}. \tag{15}$$

A well-known result in elementary number theory states that if $p>p_0$, then the number of solutions of the congruence

$$x^k + y^k \equiv a \pmod{p^k}, \qquad x,\ y \not\equiv 0 \pmod{p}$$

is greater than $p^k/2$.

Now observe that the number of solutions of the congruence (15) in residues where at least one of them does not satisfy (9) is less than $p_j^k/4$. To see this observe that there are at most $p_j^k/8k$ residues not satisfying (9), and once one such residue has been chosen there are at most $k$ choices for the other residue in (15). Thus the number of solutions of (15) in residues satisfying (9) is greater than $p_j^k/4k$. Hence by (9) the number of solutions in $a_{k-1}$ and $a_k$ of (15) is greater than

$$\left(\frac{l}{sT_r p_j^{k-1}}\right)^2 \frac{p_j^k}{4} = \frac{l^2}{4s^2 T_r^2 p_j^{k-2}}. \tag{16}$$

From (14) and (16) we have

$$F_j(T_r) > l^k T_r^{-k} s^{-2} (100k)^{-k}. \tag{17}$$

Thus from (17) and (11) and $l>c_1 n$ we have, for $r>r_0(k, s, c_1)$,

$$F(T_r) > r(lT_r^{-1}(100k)^{-1})^k s^{-2} > r^{1/2}(n^k/T_r^k). \tag{18}$$

Now the integers $\sum_{i=1}^{k} a_i^k$ are all less than $kn^k$. Thus there are at most $kn^k T_r^{-k}$ of them which are multiples of $T_r^k$ and hence by (18) for at least one of these integers, say $m_1 T_r^k$, the number of solutions of

$$m = m_1 T_r^k = \sum_{i=1}^{k} a_i^k$$

is greater than $r^{1/2}/k > t$ for $r > t^2k^2$, and this completes the proof of our theorem.

Now we 'only' have to prove the existence of an integer $T_r$ satisfying (8) and (9) and this will be the chief difficulty of our proof. We need three lemmas.

LEMMA 1. *Let $\varepsilon > 0$, $c > 0$, and $r$ be a positive integer. Then there is an $n_0 = n_0(\varepsilon, c, r)$ so that for every $n > n_0$ if $1 < a_1 < \ldots < a_l < n$, $l > cn$ is any sequence of integers, then there is a square-free integer $t_r < t_0(\varepsilon, c, r)$ so that $V(t_r) = r$ ($V(m)$ denotes the number of distinct prime factors of $m$) and for every divisor $d$ of $t_r$,*

$$(1-\varepsilon)\, l/d < A(0, d; n) < (1+\varepsilon)\, l/d. \tag{19}$$

The proof of the lemma follows fairly easily from Turán's method and we will leave some of the details to the reader. First of all it immediately follows from Turán's method that

$$\sum \frac{1}{p} < C_1, \qquad C_1 = C_1(\varepsilon, c) \tag{20}$$

where in $\sum 1/p$ the summation is extended over all the primes $p$ which do not satisfy

$$\frac{(1-\varepsilon/r)\, l}{p} < A(0, p; n) < \frac{(1+\varepsilon/r)\, l}{p}. \tag{21}$$

Henceforth we only consider primes $p$ which satisfy (21). Let $p_1$ be the smallest such prime. Put $t_1 = p_1$; $t_1$ clearly satisfies (19). Suppose we have already constructed an integer $t_s = p_1 \cdots p_s$, $p_1 < \cdots < p_s$ so that for every divisor $d'$ of $t_s$ we have

$$(1-\varepsilon_s/r)\, l/d' < A(0, d'; n) < (1+\varepsilon_s/r)\, l/d'. \tag{22}$$

It again follows by Turán's method (taking note of (22)) that

$$\sum{}' 1/p < C_{s+1} \tag{23}$$

where in $\sum 1/p$ the summation is extended over the primes $p$ for which for some divisor $d'$ of $t_s$,

$$(1-\varepsilon_{(s+1)}/r) l/pd' < A(0, pd'; n) < (1+\varepsilon_{(s+1)}/r) l/pd' \tag{24}$$

does not hold. Let $p_{s+1}$ be the smallest prime greater than $p_s$ which satisfies (24) for every divisor $d'$ of $t_s$. Put $t_{s+1} = t_s p_{s+1}$. Clearly $t_r$ satisfies (19) and by our construction $t_r < t_0(\varepsilon, c, r)$ which proves our lemma.

LEMMA 2. *Let $\varepsilon>0$, $c>0$, $m_1<\cdots<m_r$ be any sequence of integers which are pairwise relatively prime. Let $L>L_0(c,\varepsilon)$, $N>N_0(m_r, L, \varepsilon)$ and $b_1<\cdots<b_l<N$, $l>cN$ be any sequence of integers. An $m_i$, $1\leqq i\leqq r$, is said to be bad if there are more than $\varepsilon m_i$ residue classes $u \pmod{m_i}$ so that for each of them*

$$B(u, m_i, N)<l/2Lm_i. \tag{25}$$

*Then there are fewer than L bad $m_i$'s.*

The lemma would follow easily from the large sieve but we give a very simple direct proof. A residue class $u \pmod{m_i}$ is bad if it satisfies (25). If a $b_j$ is congruent to a bad residue class $\bmod m_i$ for any $i=1,\ldots,r$, we throw it away. Assume that our lemma is not true and that there are $L$ or more bad $m_i$'s. Consider any $L$ of them, say $m_{i_1},\ldots,m_{i_L}$. We throw away, by (25), at most $l/2$ $b$'s; thus by $l>cN$ there are at least $l/2$ $l$'s, $b_1<\cdots<b_M$, so that every $b_j \pmod{m_{i_s}}$, $1\leqq s\leqq L$ is not a bad residue class (i.e. $B(b_j, m_{i_s}, N)$ does not satisfy (25)). But since $m_{i_s}$ is bad, $1\leqq s\leqq L$, there are at least $\varepsilon m_{i_s}$ bad residues $\bmod m_{i_s}$, or the $b$'s are in at most $(1-\varepsilon)^L \prod_{s=1}^{L} m_{i_s}$ residue classes mod $\prod_{s=1}^{L} m_{i_s}$. Thus for $L>L_0(c,\varepsilon)$,

$$cN/4<l/2<M<(1+o(1))\,(1-\varepsilon)^L\, N<cN/4,$$

an evident contradiction, which proves Lemma 2.

Let now $t_r$ be an integer which satisfies (19) and let $r$ be sufficiently large. Let $d \mid t_r$. A prime $p \mid t_r/d$ is said to be bad with respect to $d$ if the following holds: Let $b_1<\cdots<b_r<n/d$ be the integers $a_i/d$, $r>(1-\varepsilon)\, l/d>(1-\varepsilon)\, cn/d$, by Lemma 1. Now $p$ is bad (with respect to $d$) if there are more than $\varepsilon p^k$ residues $\bmod p^k$ so that (25) holds for each of them ($m_i=p^k$, $N=n/d$). By Lemma 2 there are fewer than $L$ bad primes $p \mid t_r/d$.

LEMMA 3. *There is a $d \mid t_r$, $V(d)>\log r/2\log 2$ so that no $p \mid d/d_1$ is bad with respect to $d_1$ where $d_1$ is any divisor of $d$.*

If we prove Lemma 3 our proof is finished since we can simply put $d=T_r$ and (8) and (9) are satisfied. Thus we only have to prove Lemma 3.

Lemma 3 follows from an argument used by Spencer and Erdös (their paper will be soon published in *Matematikai Lapok*) but in view of the fact that the paper is in Hungarian it seems appropriate to give the simple proof in full detail. The argument is of course purely combinatorial. Let $|\varphi|=r$, $\varphi_1\subset\varphi$. By assumption there are fewer than $L$ bad elements $x\in\varphi$ with respect to $\varphi_1$ ($x\notin\varphi_1$). A subset $\varphi_1$ of $\varphi$ is called bad if there is an element $x$ of $\varphi_1$ so that $x$ is bad with respect to $\varphi_1-x$. Clearly there are at most $L\binom{r}{u-1}$ bad subsets $\varphi_1\subset\varphi$ with $|\varphi_1|=u$.

We want to prove that there is a subset $A \subset \varphi$, $|A| > \log r/2 \log 2$ which contains no bad subsets, and this will complete the proof of our lemma.

Clearly there are at most

$$\sum_{u=1}^{l} \binom{r-u}{l-u} L \binom{r}{u-1} < lL \frac{r^{l-1}}{(l-1)!} 2^l$$

$l$-element subsets of $\varphi$ which contain a bad subset. Now if $r > r_0(L)$, $l \leqq \log r/2 \log 2$, then

$$lL \frac{r^{l-1}}{(l-1)!} 2^l < \binom{r}{l};$$

thus there is an $l$-element subset $A$, $l \geqq \log r/2 \log 2$, which contains no bad subset, which proves our lemma and theorem.

Lemma 1 could have been strengthened in the following way:

Instead of (19) we could have proved that for every $u$,

$$(1-\varepsilon)\, l/d < A(u, d; n) < (1+\varepsilon)\, l/d \tag{19'}$$

uniformly for every residue class $u$.

The proof would be essentially the same as that of (19). Several other possibilities of generalisations we plan to discuss in another paper.

## REFERENCES


**1.** S. Chowla, Indian Phys.-Math. J. **6** (1935), 65–68.

**2.** H. Davenport, *Sums of three positive cubes*, J. London Math. Soc. **25** (1950), 339–343. MR **12**, 393.

**3.** P. Erdös, *On the representation of an integer as the sum of k k-th powers*, J. London Math. Soc. **11** (1936), 133–136.

**4.** P. Erdös and K. Mahler, *On the number of integers which can be represented by a binary form*, J. London Math. Soc. **14** (1939), 134–139.

**5.** P. Erdös, *On the sum and difference of squares of primes*. I, II, J. London Math. Soc. **12** (1937), 133–136, 168–171.

**6.** B. Lindström, *An inequality for $B_2$-sequences*, J. Combinatorial Theory **6** (1969), 211–212.

**7.** K. Mahler, *Note on the hypothesis k of Hardy and Littlewood*, J. London Math. Soc. **11** (1936), 136–138.

***8.** ———, *On the lattice points on curves of genus* 1, Proc. London Math. Soc. **39** (1935), 431–466.

**9.** J. Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc. **43** (1938), 377–385.



MATHEMATICAL INSTITUTE OF THE HUNGARIAN ACADEMY OF SCIENCE
BUDAPEST, HUNGARY


* P. Erdös remembers that Mahler in a later paper improved the exponent $\frac{1}{4}$ to 2 but is unable to trace the reference.