Extremal Problems in Number Theory

BY

P. ERDÖS

I would like to illustrate the problems which I shall investigate in this paper by an example. Denote by $r_k(n)$ the maximum number of integers not exceeding n, no k of which form an arithmetic progression. The problem is to determine or estimate the value of $r_k(n)$. This problem is connected with several known questions of number theory. If $r_k(n) < (1-\epsilon)n/\log n$ for every k, if n is sufficiently large, then the prime number theorem implies that for every k there are k primes in arithmetic progression. $r_k(n) < n/2$ would imply the well known theorem of Van der Waerden. The first paper on $r_k(n)$ is due to Turán and myself [2]. The best bounds for $r_3(n)$ presently known are [1;7]

$$n^{1-c_1/\sqrt{\log n}} < r_3(n) < c_2 n/\log\log n.$$

It is not even know if $r_4(n) = o(n)$.

Some of these extremal problems lead to interesting and deep questions in number theory, others are mere exercises. Recently I published in Hungarian a paper entitled *Extremal problems in number theory* (Mat. Lapok **13**(1962), 228-255).[1] The present paper consists of a discussion of somewhat unrelated extremal problems. In the first part of this paper I will give a short resume of the principal results of my Hungarian paper and in the second part I will give in more detail some recent results which L. Moser and I found jointly during my recent visit at the University of Alberta.

1. An old conjecture of Turán and myself [3] states that if $a_1 < a_2 < \cdots$ is an infinite sequence of integers and $f(n)$ denotes the number of solutions of $n = a_i + a_j$ then $f(n) > 0$ for $n > n_0$ implies

$$\limsup_{n=\infty} f(n) = \infty. \tag{1}$$

More generally it can be conjectured that (1) follows from $a_k < ck^2$ ($k = 1, 2, \cdots$). These conjectures seem very deep. I can prove the multiplicative analog of (1). Let $a_1 < a_2 < \cdots$ and denote by $g(n)$ the number of solutions of $n = a_i a_j$. Then $g(n) > 0$ for $n > n_0$ implies

$$\limsup_{n=\infty} g(n) = \infty. \tag{2}$$

[1] If a result is stated without any reference, a reference to this paper is intended.

In fact (2) follows from the following weaker hypothesis. Let $A(x)=\sum_{a_i<x}1$. Assume that for every k

$$\limsup_{x=\infty} A(x)\left(x\left(\frac{\log\log x}{\log x}\right)^k\right)^{-1}=\infty.$$

Then (2) follows.

The proof of these statements is difficult and has not yet been published. The following question can be considered: Let $a_1<a_2<\cdots<a_z\leqq n$ be a sequence of integers so that the products

$$\prod_{i=1}^{z} a_i^{\epsilon_i},\quad \epsilon_i=0 \quad\text{or}\quad 1 \tag{3}$$

are all distinct. What is the maximum of z? I proved that $z<\pi(n)+2n^{2/3}$ and it seems likely that $z<\pi(n)+cn^{1/2}/\log n$. We obtain a completely different question if instead of (3) we assume that

$$\prod_{r=1}^{l_1} a_{i_r}=\prod_{r=1}^{l_2} a_{j_r} \tag{4}$$

can hold only if $l_1=l_2$. This condition is clearly satisfied if the a's are the numbers $\equiv 2 \pmod 4$. Perhaps here max $z>n(1-\epsilon)$ for every $\epsilon>0$ if $n>n_0$. Selfridge recently pointed out that max $z>(n/e)(1-\epsilon)$. To see this let $p_1<p_2<\cdots<p_k$ be a sequence of large primes with $\sum_{i=1}^{k} 1/p_i=1+o(1)$ and the a's are the numbers of the form

$$p_i t,\quad 1\leqq i\leqq k,\qquad \left(\prod_{i=1}^{k} p_i, t\right)=1.$$

2. A system of congruences

$$a_i \pmod{n_i},\quad n_1<\cdots<n_k \tag{5}$$

is called a covering system [4] if every integer is satisfied by at least one of the congruences (5). It is not known if the value of n_1 can be arbitrarily prescribed nor is it known whether all the n_i can be odd. S. Stein calls a system (5) disjoint if every integer satisfies at most one of the congruences (5). He conjectured for every disjoint system (5) there is a u satisfying

$$0<u\leqq 2^k,\quad u\not\equiv a_i \pmod{n_i},\quad 1\leqq i\leqq k. \tag{6}$$

I proved (6) with $k2^k$ instead of 2^k by showing that for every disjoint system (5)

$$\sum_{i=1}^{k}\frac{1}{n_i}\leqq 1-\frac{1}{2^k}, \tag{7}$$

and (7) is easily seen to be best possible.

Perhaps the following stronger conjecture holds: Let

(8) $$a_i \pmod{n_i}, \quad 1 \leqq i \leqq k,$$

be a system of congruences ($n_{i_1} \neq n_{i_2}$ is not assumed) such that there is an integer u for which $u \not\equiv a_i \pmod{n_i}$, $1 \leq i \leq k$. Then such a u exists satisfying $0 < u \leqq 2^k$. I can only show that such a u exists satisfying $0 < u \leqq A(k)$ but I cannot give an explicit estimation for $A(k)$.

Finally Stein and I considered the following question: Let $a_i \pmod{n_i}$, $n_1 < \cdots < n_k \leqq x$ be a disjoint system of congruences. What is the maximum value of k? Put max $k = f(x)$. We conjectured that

(9) $$\lim_{x=\infty} f(x)/x = 0$$

but were unable to prove (9). We proved that for every $\epsilon > 0$ and $x > x_0(\epsilon)$

$$f(x) > x/\exp((\log x)^{1/2+\epsilon}).$$

3. Denote by $h(n,k)$ the maximum number of integers not exceeding n from which one cannot select $k+1$ integers which are pairwise relatively prime. Denote by $A(n,k)$ the number of integers not exceeding n which are multiples of at least one of the first k primes $2, 3, \cdots, p_k$. It seems likely that

(10) $$h(n,k) = A(n,k).$$

It is easy to prove (10) for $k = 1$ and not hard to prove it for $k = 2$ but for larger values of k the proof seems more complicated and I have not been able to prove (10) for all values of k.

4. What is the maximum number of integers not exceeding n so that the least common multiple of any two of them does not exceed n? I conjecture that the extremal sequence is given by the numbers $1 < i < (n/2)^{1/2}$ and $(n/2)^{1/2} \leqq 2j \leqq (2n)^{1/2}$.

5. What is the largest $k = k(n)$ for which there is an $m \leqq n$ so that each of the integers $m+i$, $1 \leqq i \leqq k$, are divisible by at least one prime $> k$? It is not hard to prove that

$$k(n) > \exp(\log n)^{1/2-\epsilon}.$$

It seems likely that $k(n) = o(n^\epsilon)$, but I have not been able to obtain any non-trivial upper bound for $k(n)$.

In the second part of this paper I now give some results together with their proofs which we obtained jointly with L. Moser. Let $a_1 < a_2 < \cdots < a_k$ be k distinct real numbers. Denote by $f(n; a_1, a_2, \cdots, a_k)$ the number of solutions of

(11) $$n = \sum_{i=1}^{k} \epsilon_i a_i, \; \epsilon_i = 0 \quad \text{or} \quad 1,$$

and put

$$F(k) = \max_{n, a_1, \cdots, a_k} f(n; a_1, \cdots, a_k).$$

(If we had not assumed that the a's are all distinct but only that $a_i \neq 0$ then we would have easily obtained that $F(k) = C_{k,[k/2]}$.)

It seems likely that $f(n; a_1, \cdots, a_k)$ assumes its maximum if $n=0$ and the a's are $0, \pm 1, \pm 2, \cdots$. In other words

$$F(k) = f\left(0; -\left[\frac{k}{2}\right], -\left[\frac{k-2}{2}\right], \cdots, 0, 1, \cdots, \left[\frac{k-1}{2}\right]\right), \tag{12}$$

but we have not been able to prove (12). It may be possible to obtain an explicit formula for the right side of (12) but we have not succeeded in doing so. It is easy to see that

$$F(k) > c_1 2^k / k^{3/2}$$

and in fact it is not hard to show that the right side of (12) is $> c_1 2^k / k^{3/2}$. We conjecture that

$$F(k) < c_2 2^k / k^{3/2}. \tag{13}$$

A still sharper conjecture than (13) would be that the number of solutions of

$$n = \sum_{i=1}^{k} \epsilon_i a_i, \qquad \sum_{i=1}^{k} \epsilon_i = t, \qquad \epsilon_i = 0 \quad \text{or} \quad 1$$

is less than $c_3 2^k / k^2$ (c_3 is independent of t). We were unable to prove (13), but prove the weaker

THEOREM 1.

$$F(k) < c_4 2^k \left(\frac{\log k}{k}\right)^{3/2}.$$

First we prove a Lemma: Let $b_1 < b_2 < \cdots < b_m$ be such that no b equals the sum of any number of other b's; then for every n

$$f(n; b_1, \cdots, b_m) < c_5 2^m / m^{3/2}.$$

Denote by $B_1, \cdots, B_t$ the set of those b's for which

$$\sum_{b_i \in B_j} b_i = n. \tag{14}$$

We have to show

$$t < c_5 2^m / m^{3/2}. \tag{15}$$

First of all we can restrict ourselves to those B's which contain more than $[m/4]$ b's since by a simple and well known computation we obtain that the number of B's containing at most $[m/4]$ b's is at most

$$\sum_k \binom{m}{k} = o(2^m / m^{3/2}), \quad 0 \leq k \leq \left[\frac{m}{4}\right], \tag{16}$$

in fact the sum in (16) is less than $(2-c)^m$ for a fixed $c > 0$.

Denote by $B_1, \cdots, B_{t_1}$ the B's satisfying (14) which have more than $[m/4]$ elements. To prove (15) it will suffice to show

(17) $$t_1 < c_6 2^m / m^{3/2}.$$

Denote by $D_1, \cdots, D_l$ the set of all subsets of B_i, $1 \leqq i \leqq t_1$ which we obtain from B_i by omitting one $b \in B_i$ in all possible ways. All these D's are distinct for if $D_j \cup b_1 = D_j \cup b_2$ then by (14) $b_1 = b_2$. Thus since we obtain more than $(m/4)$ D's from every B, we have

(18) $$l > \frac{mt_1}{4}.$$

Next we show that one D cannot contain any other. Assume to the contrary that $D_1 \subset D_2$ and say $D_1 \subset B_1$, $D_2 \subset B_2$ $(B_1 \neq B_2)$, and $B_1 = D_1 \cup b_1$, $B_2 = D_2 \cup b_2$. Put

(19) $$D_2 = D_1 \cup b_3 \cup \cdots \cup b_r.$$

Then by (14) and (19)

$$b_1 = b_2 + b_3 + \cdots b_r$$

which contradicts the hypothesis of the Lemma.

By a well-known theorem of Sperner [**9**] we obtain

(20) $$l \leqq \binom{m}{[m/2]};$$

(17) now follows from (18) and (20), hence our Lemma is proved.

Now we prove Theorem 1. Without loss of generality we can assume that at least $[k/2]$ of the a's are positive. We now distinguish two cases. In the first case there is a $u > 0$ so that there are at least $c_7 k/\log k$ a's satisfying

(21) $$u \leqq a_1 < a_2 < \cdots < a_s < 2u, \ s = [c_7 k/\log k].$$

Then clearly no a_r, $1 \leqq r \leqq s$ is a sum of other a_j's, $1 \leqq j \leqq s$. Denote by $a_{s+1}, \cdots, a_k$ the other a's and consider

(22) $$n = \sum_{i=1}^{k} \epsilon_i a_i = \sum_{i=1}^{s} \epsilon_i a_i + \sum_{s+1}^{k} \epsilon_i a_i.$$

We have 2^{k-s} choices for $\sum_{i=s+1}^{k} \epsilon_i a_i$, and once $\sum_{i=s+1}^{k} \epsilon_i a_i$ has been chosen we must determine $\sum_{i=1}^{s} \epsilon_i a_i$ so that

(23) $$\sum_{i=1}^{s} \epsilon_i a_i = n - \sum_{i=s+1}^{k} \epsilon_i a_i.$$

But by our Lemma (23) has at most $c_5 2^s / s^{3/2}$ solutions, which proves Theorem 1 in case I.

Assume next that (21) holds for no u. Then there are at least $\log k / c_7$ disjoint intervals $(u_i, 2u_i)$ which contain at least one a_i. But then clearly there is a sequence

$$a_1 < a_2 < \cdots < a_j, \quad j \geqq \frac{\log k}{2c_7}, a_{i+1} > 2a_i, 1 \leqq i < j-1. \tag{24}$$

We obtain a sequence satisfying (24) by considering the disjoint intervals $(u_i, 2u_i)$, $1 \leqq i \leqq \log k/c_7$ and taking a_i to satisfy $u_{2i-1} \leqq a_i < u_{2i}$. From (24) it follows that the sums

$$\sum_{i=1}^{j} \epsilon_i a_i \tag{25}$$

are all distinct. As in case I we write

$$n = \sum_{i=1}^{j} \epsilon_i a_i + \sum_{j+1}^{k} \epsilon_i a_i. \tag{26}$$

We have 2^{k-j} choices for $\sum_{i=j+1}^{k} \epsilon_i a_i$, but once $\sum_{i=j+1}^{k} \epsilon_i a_i$ has been chosen there is at most one choice for $\sum_{i=1}^{j} \epsilon_i a_i$, hence (14) has at most

$$2^{k-j} < 2^k/k^2$$

solutions for suitable choice of c_7. This completes the proof of Theorem 1.

It would have been easy to give an explicit inequality for c_4. We have refrained from doing this, since Theorem 1 probably does not give the right order of magnitude for $F(k)$.

Theorem 1 clearly remains true if the a's are distinct complex numbers and in fact vectors of a finite dimensional euclidean space. It is not clear if it remains true if the a's are vectors in Hilbert space. If the a's are distinct elements of an abelian group the above proof gives $F(k) < c2^k/k$ (since the D's are distinct here too). Here this result is in general best possible as is shown if the a's are the residue classes (mod k).

Trying to improve Theorem 1 led us to a few questions of independent interest. Let $a_1, a_2, \cdots, a_n$ be n real numbers all different from 0. Denote by $f(n)$ the largest integer so that for every sequence $a_1, \cdots, a_n$ one can always select $k = f(n)$ of them $a_{i_1}, \cdots, a_{i_k}$ so that

$$a_{i_{j_1}} + a_{i_{j_2}} \neq a_{i_{j_3}}, \qquad 1 \leqq j_1 \leqq j_2 < j_3 \leqq k. \tag{27}$$

THEOREM 2.

$$f(n) \geqq \frac{n}{3}.$$

The proof is very simple. Denote by I_r the set in $\alpha, 0 < \alpha < T, T$ large for which $a_r\alpha$ (mod 1) is between $1/3$ and $2/3$, $m(I_r)$ denotes the measure of I_r. We evidently have

$$\left| m(I_r) - \frac{1}{3} \right| < A \tag{28}$$

where A is independent of T. It may depend on the a's. From (28) it clearly follows that there is an α so that for at least $(n/3)$ a's $a_{i_r}\alpha \pmod 1$, $1 \leqq r \leqq n/3$, is between $1/3$ and $2/3$. Clearly these a's satisfy (27), which proves Theorem 2.

Can Theorem 2 be improved? The sequence $1, 2, \cdots, n$ shows that in any case $f(n) \leqq \lfloor (n+2)/2 \rfloor$ and if we permit $j_1 = j_2$ in (27) then

$$f(n) \leqq \frac{3}{7} n.$$

PROOF. Consider the numbers $2, 3, 4, 5, 6, 8, 10$. It is readily verified that one cannot choose 4 of these without choosing one which is the difference of two others. Now consider the above 7 numbers each multiplied by 10^r, $r = 1, 2, \cdots, k$. We then have $7k$ numbers from which at most $3k$ can be chosen. This construction is essentially due to D. Klarner. An independent example giving a slightly weaker result was obtained earlier by A. J. Hilton.

If in (27) we exclude $j_1 = j_2$ then perhaps $f(n) = [(n+2)/2]$. It is surprising that this simple question seems to present considerable difficulties, but perhaps we overlook the obvious.

Theorem 2 holds for any finite Abelian group, perhaps it holds for a non-Abelian group too (perhaps with a different constant than $1/3$). An analogous theorem also holds for measurable sets of real numbers and probably holds under more general conditions. It can be shown that $1/3$ is the best possible constant for measurable sets (mod 1) or for residues (mod p).

Denote by $\phi(n)$ the largest integer so that if $a_1, a_2, \cdots, a_n$ are n distinct real numbers one can always find $\phi(n)$ of them $a_{i_1}, \cdots, a_{i_k}$, $k = \phi(n)$ so that $a_{i_j} + a_{i_l} \neq a_r$, $1 \leqq j < l \leqq k$, $1 \leqq r \leqq n$. To obtain a nontrivial result it is necessary to assume here $j \neq l$, for otherwise $a_i = 2^i$, $1 \leqq i \leqq n$ would imply $\phi(n) = 1$. We showed $\phi(n) \to \infty$ as $n \to \infty$ and a remark by Klarner implies that

$$\phi(n) > c \log n.$$

We do not give proofs since these estimates for $\phi(n)$ are probably very far from its true order of magnitude. A simple example shows that $\phi(n) < (n/3) + O(1)$. To see this let the a's be the following $3m$ numbers:

$$2^{k+2} - 1, 2^{k+2}, 2^{k+2} + 1, \qquad 0 \leqq k \leqq m - 1.$$

Clearly from each triplet $2^{k+2} - 1, 2^{k+2}, 2^{k+2} + 1, 0 \leqq k \leqq m - 2$ one can choose only one a_{i_j}. Thus $\phi(3m) \leqq m + 2$.

J. L. Selfridge has improved this to $\phi(n) < (1/4 + \epsilon)n$ by considering

$$2^k + m, \qquad m = 0, \pm 1, \cdots, \pm t.$$

It seems likely that $\phi(n) = o(n)$.

A possible generalization would be the following result: To every k there is an $n_0 = n_0(k)$ so that if $n > n_0(k)$ and $a_1, a_2, \cdots, a_n$ are n elements of a group so that none of the products $a_i a_j$ equal the unit element then there are

k a's $a_{i_1}, \cdots, a_{i_k}$ so that all the products $a_{i_{j_1}} a_{i_{j_2}}$ differ from all the a_r's, $1 \leqq r \leqq n$. We have not shown this even for $k=3$ (compare a result of L. Moser [6]).

Denote by $g(n)$ the largest integer so that from any set of n real numbers $a_1, \cdots, a_n$ one can always select $g(n)=k$ of them $a_{i_1}, \cdots, a_{i_k}$ so that no a_{i_k} is the sum of other a_{i_j}'s. Denote by $k(n)$ the largest integer k so that from n real numbers $a_1, \cdots, a_n$ one can always find k of them $a_{i_1}, \cdots, a_{i_k}$ so that two sums

$$\sum_{j=1}^{l_1} a_{i_j} = \sum_{s=1}^{l_2} a_{i_s} \tag{29}$$

can hold only if $l_1 = l_2$. By the same method as we used in the proof of Theorem 2 we can show

$$g(n) \geqq \sqrt{(n/2)} \tag{30}$$

and

$$h(n) \geqq n^{1/3}. \tag{31}$$

In the proof of (30) I_r is the set for which $a_r\alpha$ (mod 1) is between $1/\sqrt{(2n)}$ and $\sqrt{(2/n)}$, in the proof of (31) I_r is the set for which $a_r\alpha$ (mod 1) is between $1/n^{1/3} - 1/2n^{2/3}$ and $1/n^{1/3} + 1/2n^{2/3}$. (30) and (31) are probably far from being best possible. It is known that $h(n) < c_8 n^{5/6}$ [**5**] and by complicated arguments we can show that $g(n) = o(n)$, very likely $g(n) < n^{1-c_9}$ for some $c_9 > 0$.

It is not difficult to show that if $a_1, \cdots, a_n$ are given numbers one can always find $a_{i_1}, \cdots, a_{i_k}$, $k \geqq [\log n / \log 3]$, so that all the sums $\sum_{r=1}^{k} \epsilon_r a_{i_r}$ are different for $\epsilon_i = 0$ or 1. Perhaps this can be improved to $k \geqq [\log n / \log 2]$. The example $a_i = i, 1 \leqq i \leqq n$ shows that this result if true is nearly best possible. The bound (31) cannot be generalized to measurable sets, since it easily follows from the density theorem of Lebesgue that (29) is satisfied in every set of positive measure. On the other hand it is easy to see that every set of real numbers of positive measure contains a subset of positive measure no element of which is the sum of any others (we simply take the intersection of our set with the interval $(2^k, 2^{k+1})$ for some suitable k), but it is not clear whether it is possible to give a lower bound for the measure of such sets.

Denote finally by $H(n)$ the smallest integer so that we can split the integers $1 \leqq m \leqq n$ into $H(n)$ classes $(\mathscr{C}_i, 1 \leqq i \leqq H(n))$ so that the equation $x+y=z, x, y, z$ in $\mathscr{C}_i$ is unsolvable for every $1 \leqq i \leqq H(n)$. Schur [**8**] proved that $H(cn!) > n$. It seems very hard to decide whether $H(n) > c \log n$ holds for a certain $c > 0$. Define $H^*(n)$ as the smallest integer so that one can split the integers $1 \leqq m \leqq n$ into $H^*(n)$ classes $\mathscr{C}_i, 1 \leqq i \leqq H^*(n)$, so that no element of $\mathscr{C}_i$ $(1 \leqq i \leqq H^*(n))$ is the sum of distinct elements of $\mathscr{C}_i$. Here $H^*(n) > c \log n$ follows immediately from [**5**]

$$\sum_{a_j \in \mathscr{E}_i} \frac{1}{a_j} < 103.$$

We have not been able to determine $H^*(n)$ or even to prove that $\lim_{n=\infty} H^*(n)/\log n$ exists.

ADDITIONS. Several of the problems which were stated as unsolved in the above paper have been settled in the meantime. First of all I refer to some of my papers which I have published since then on this and related subjects.

P. Erdös, *Problems and results on combinatorial number theory*. I, II, II′, and III.

I. *A survey of combinatorial theory* (J. N. Srivastava, Editor), North-Holland, Amsterdam, 1973, pp. 117–138.

II. Journée d'Arithmétique Bordeaux, 1974.

II′. Indian J. Math. **40** (1976), 285–298.

III. *Number theory day* (Proc. Conf., Rockefeller Univ., 1976), Lecture Notes in Math., vol. 626, Springer-Verlag, Berlin and New York, pp. 43–73. (I apologize for II and II′, I made the wrong references.)

P. Erdös, *Some extremal problems in combinatorial number theory*, Mathematical Essays Dedicated to A. J. Macintyre (H. Shankar, Editor), Ohio Univ. Press, Athens, Ohio, 1970, pp. 123–133. MR **43** #1942.

Now I list the progress made on the problems stated in my paper.

Szemerédi proved our conjecture with Turán $r_k(n) = o(n)$; Fürstenberg obtained another proof using ergodic theory.

E. Szemerédi, *On sets of integers containing no k elements in arithmetic progression*, Acta Arith. **27** (1975), 199–245.

Fürstenberg, *Ergodic behaviour of diagonal measures and a theorem of Szemerédi*, J. Analyse Math. **31** (1977), 204ff.

The proof of (2) appeared in the meantime (P. Erdös, *On the multiplicative representation of integers*, Israel J. Math. **2** (1964), 251–261).

Now let us consider (3). I proved the conjecture

$$Z < \pi(n) + cn^{1/2}/\log n.$$

P. Erdös, *Remarks on number theory*. V, Extremal Problems in Number Theory. II, Mat. Lapok., 1965. (Hungarian)

With respect to (4) I. Ruzsa proved that $Z < n(1 - \varepsilon)$ holds if $\varepsilon < 0$ is a sufficiently small constant. His proof is not yet published.

(5) is still open–the best result is due to Choi, he proved that $n_1 = 20$ is possible. S. L. G. Choi, *Covering the set of integers by congruence classes of distinct moduli*, Math. Comp. **25** (1971), 885–895.

(6) and (8) have been settled by Selfridge and independently by R. B.

Crittenden and C. L. Vanden Zynden, *Any n arithmetic progressions covering the first 2^n integers cover all integers*, Proc. Amer. Math. Soc. **24** (1970), 475–481.

Szemerédi and I proved (9); in fact we proved a somewhat stronger result.

P. Erdös and E. Szemerédi, *On a problem of Erdös and Stein*, Acta Arith. **15** (1968), 85–90.

The problem stated in §4 (p. 183) is still open. For a partial result see S. L. G. Choi, *The largest subset in* $(1, n)$ *whose integers have pairwise l.c.m. not exceeding* n, Acta Arith. **29** (1976), 105–111.

The conjecture (13) has been proved by Sárközy and Szemerédi, *Über ein Problem von Erdös and Moser*, Acta Arith. **11** (1965–66), 205–208.

The conjecture (2) is still open, see J. H. van Lint, *Representation of* 0 *as* $\Sigma_{k=-N}^{N}\varepsilon_k k$, Proc. Amer. Math. Soc. **18** (1967), 182–184.

Many of the problems stated at the end of the paper have been investigated in a more general form, under the heading of sum free sets, by Diananda, Yap, Ann Penfold Street and others. See the book by W. D. Wallis, Ann Penfold Street and Jennifer Sebessy Wallis, *Combinatorics: Rome squares, sum free sets, Hadamard matrices*, Lecture Notes in Math., vol. 292, Springer-Verlag, Berlin and New York, 1972.

Several of the problems stated were settled (or the old results improved) by Choi. He proved $\phi(n) < en/\log n$ (see p. 187).

Choi improved (31) to $h(n) > en^{1/3} \log n$ (on p. 188, lines 4–6, $h(n)$). Strauss proved $h(n) < c\sqrt{n}$.

S. L. G. Choi, *On an extremal problem in number theory*, J. Number Theory **6** (1974), 109–112; *On sequences not containing a large sum-free subsequence*, Proc. Amer. Math. Soc. **41** (1973), 437–440; *The largest sum-free subsequence from a sequence of numbers*, ibid. **39** (1973), 42–44; *Problems and results on finite sets of integers*, Finite and Infinite Sets, vol. 10, Colloq. Math. Soc. János Bolyai, (Keszthely, Hungary, 1973), North-Holland, Amsterdam, 1975, pp. 269–273. MR **51** #5544.

E. Straus, *On a problem in combinatorial number theory*, J. Math. Sci. **1** (1966), 77–80.

References

1. F. A. Behrend, *On sets of integers which contain no three terms in arithmetical progression*, Proc. Nat. Acad. Sci. U. S. A. 32(1946), 331-332.

2. P. Erdös and P. Turán, *On some sequences of integers*, J. London Math. Soc. 11(1936), 261-264.

3. ——, *On the problem of Sidon in additive number theory and on some related problems*, ibid 16(1941), 212-215; see also A. Stöhr, *Gelöste und ungelöste Fragen über basen der natürlichen Zahlenreihe*. I, II, J. Reine Angew. Math. 194(1955), 40-65 and 111-140.

4. P. Erdös, *On a problem on systems of congruences*, Mat. Lapok 4(1952), 122-128 (Hungarian); see also S. K. Stein, *Unions of arithmetic sequences*, Math. Ann. 134(1958), 289-294.

5. ——, *Remarks in number theory*. III. *Some problems in additive number theory*, Mat. Lapok **13**(1962), 28-38. (Hungarian)

6. L. Moser, *Advanced problem* 4317, Amer. Math. Monthly **57**(1950), 345.

7. K. F. Roth, *On certain sets of integers*, J. London Math. Soc. **28**(1953), 104-109.

8. I. Schur, Jber. Deutsch. Math.-Verein. **25**(1916), 114.

9. E. Sperner, *Ein Satz über Untermengen einer endlichen Menge*, Math. Z. **27**(1928), 544-548.

UNIVERSITY OF ALBERTA