Extremal Problems in Number Theory

Paul Erdős

Hungarian Academy of Sciences

Within the last few years I have written several papers on this subject. To keep this note short I mention only two or three new problems and discuss some of the old problems where some progress has been made. I quote some of the relevant papers.

P. Erdős, On unsolved problems, Publ. Math. Inst. Hung. Acad. 6(1961), 221-254, see also Michigan Math. Journal (1957).

P. Erdős, Some recent advances and current problems in number theory, T. L. Saaty, Lectures on Modern Math. Vol. 3, 196-244.

P. Erdős, Extremal problems in number theory, Theory of numbers, Symposia in Pure Math. VIII (1965), 181-189 (Amer. Math. Soc.). Several problems stated there were partially solved by Choi see e.g. S. L. G. Choi, On a combinatorial problem in number theory, Proc. London Math. Soc. 23(1971), 629-642.

1. Nearly fourty years ago I made the following conjecture: Let $1 \le a_1 < \ldots < a_k \le n$; $1 \le b_1 < \ldots < b_\ell \le n$ be two sequences of integers. Assume that the products $a_i b_j$, $1 \le i \le k$; $1 \le j \le \ell$ are all distinct. Then

(1) $$k\ell < c_1 n^2/\log n$$

Szemerédi recently found a surprisingly simple proof of (1), his paper will appear in the Journal of Number Theory.

It would be interesting to strengthen (1) and determine $\max k\ell$. This problem is almost certainly hopeless, but perhaps one can determine

(2) $$\lim_{n=\infty} \frac{k\ell \log n}{n^2} = c$$

It is not even quite clear that the limit in (2) exists.

Szemerédi and I proved that to every r there is an s so that in $n > n_0(r,s)$ and

(3) $$k\ell > \frac{n^2}{\log n} (\log\log n)^s$$

then for some m, $m = a_i b_j$ has more than r solutions.

The following question which just occurs to me can be raised: Let $A = \{a_1,\ldots,a_k\}$; $B = \{b_1,\ldots,b_\ell\}$ be two sequences of integers in the interval $(1,m)$. Denote by $N(A,B;n)$ the number of those integers m for which $m = a_i b_j$ has precisely one solution. Determine or estimate $\max N(A,B;n)$ where the maximum is taken over all subsequences A and B of $(1,n)$. Perhaps Szemerédi's method will help to solve this problem.

II. A long time ago Turán and I made the following conjecture: Let $1 \le a_1 < \dots < a_k \le n$ be a sequence of integers for which the sums $a_i + a_j$, $1 \le i \le j < k$ are all distinct. Then

$$\max k = n^{\frac{1}{2}} + O(1) \quad (4)$$

(4) seems very deep and I often offered and still offer 250 dollars for a proof or disproof of (4).

Until recently the sharpest result here was due to Lindstrom who proved $\max k \le n^{1/2} + n^{1/4} + 1$.

Szemerédi now improved this to $\max k \le n^{1/2} + O(n^{1/4})$. $\max k \ge (1 + o(1))\ n^{1/2}$ is an easy consequence of a theorem of Singer.

B. Lindstrom, An inequality for B_2-sequences, J. Comb. Theory 6(1969), 211-212.

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

III. Choi, Szemerédi and I recently proved that to every ℓ there is an $\varepsilon_\ell > 0$ so that if

$$1 \le a_1 < \dots < a_k \le n, \quad k > (\tfrac{2}{3} - \varepsilon_\ell)n, \quad n > n_0(\varepsilon_\ell, \ell)$$

is any sequence of integers there always are ℓ a's $a_{i_1}, \dots, a_{i_\ell}$ so that all the $\binom{\ell}{2}$ sums $a_{j_1} + a_{j_2}$ are all distinct and are elements of A (i.e., are a's).

The proof is not very difficult. It is easy to see that in this theorem $\frac{2}{3}$ cannot be replaced by any smaller number. We suspect that $\varepsilon_3 = \frac{1}{24}$, or more precisely: If $k > \frac{5n}{8} + c$ then there are three a's $a_{i_1}, a_{i_2}, a_{i_3}$ so that all the three sums $a_{i_1} + a_{i_2}, a_{i_1} + a_{i_3}, a_{i_2} + a_{i_3}$ are also a's (the three sums are trivially distinct). It is easy to see that for $k = \frac{5n}{8}$ this does not hold

Further we proved: If $k > \frac{n}{2} + n^{1-\varepsilon_\ell}$, there are ℓ integers $b_1, \ldots, b_\ell$ so that all the $\binom{\ell}{2}$ sums. $b_i + b_j$ are distinct and in A (here it is not assumed that $b_i \varepsilon A$). Also if $k = \frac{n}{2} + 2$ $n > n_0$ these are three b's b_1, b_2, b_3 so that all the sums $b_1 + b_2$, $b_1 + b_3$, $b_2 + b_3$ are a's. The odd numbers and 2 shows that this is false for $k = n + 1$. If $k > \frac{n}{2} + t$ (t independent of n) there are four b's so that the sums $b_i + b_j$, $1 \le i < j \le 4$ are all distinct and in A. We were too lazy to determine t. If $k > \frac{n}{2} + c \log n$ there are five b's so that all the ten sums $b_i + b_j$ are distinct and in A. The powers of 2 and the odd numbers show that apart from the value of c this is best possible and finally for six b's we need $k > \frac{n}{2} + c\sqrt{n}$

IV. Last year I asked the following question: Let z_i, $|z_i| < n$ be complex numbers so that the numbers $|z_i - z_j|$ differ from an integer by more than c where $0 < c < \frac{1}{2}$. Determine or estimate $t = t(c,n)$. If the z's are real the problem is trivial.

Graham and Sárközi showed that for every $c (0 < c < \frac{1}{2})$ $t > n^{\alpha_c}$ $\alpha_c (\alpha_c < \frac{1}{2})$, and Sárközi proved $t < c\, n/\log\log n$.

The same problem can clearly be posed for higher dimensions, but as far as I know has not yet been investigated.

V. Let $n + 1, \ldots, n + t$ be a sequence of consecutive composite numbers. Grimm conjectured that there are t distinct primes p_i satisfying $p_i | n + i$.

Selfridge and I proved that if Grimm's conjecture is true then $p_{i+1} - p_i < c\left(\frac{p_i}{\log p_i}\right)^{\frac{1}{2}}$ where $p_i < \ldots$ is the sequence of consecutive primes (Proceedings of the Number Theory Conference held at Pullman Washington March 1971). Thus Grimm's conjecture if true must be very deep. Selfridge and I in our paper quoted above also investigated the following question: Denote by t_n the largest value of t for which these are t_n distinct primes p_i, $1 \le i \le t_n$ so that $p_i | n + i$. We proved $t_n \ge (1 + o(1)) \log n$. Our result was improved by Ramachandra and Tjjdeman. Very recently Ramachandra and Shover proved that

$$t_n > c\left(\frac{\log n}{\log\log n}\right)^2 ,$$

which up to now is the sharpest lower bound for t_n. We have no non-trivial upper bounds for t_n.

C. A. Grimm, A conjecture on consecutive composite numbers, Amer. Math. Monthly 76(1969), 1126-1128.

VI. Let $a_1 < \ldots$ be a sequence of integers A satisfying $\sum \frac{1}{a_i} < T$. Denote by $F(A;n)$ the number of integers $m \le n$ which are not multiples of any $\underline{a}$. I conjecture that

$$F(A,n) > \frac{c\,n}{(\log n)^{\alpha_T}} \tag{5}$$

A result of Schinzel and Szekeres shows that for every $T > 1$ (5) if time is certainly best possible (except for the value of α_T).

Let us now add the assumption $(a_i, a_j) = 1$ and let $q_1, q_2, \ldots$ be the sequence of primes not exceeding n in descending order. Define ℓ by

$$\frac{1}{q_1} + \ldots + \frac{1}{q_\ell} < A < \frac{1}{q_1} + \ldots + \frac{1}{q_\ell} + \frac{1}{q_{\ell+1}} .$$

It seems to me that we have

$$F(A,n) \geq (1 + o(1)) \quad (q_1, \ldots, q_\ell; n) \tag{6}$$

Perhaps I overlook an obvious approach, but I mad no progress with (6).

A. Schinzel and G. Szekeres, Sur un problème de M. Paul Erdös, Acta Sci. Math. Szeged 20(1959), 221-229.

VII. I conjectured that if $f(n)$ is additive (i.e., $f(a,b) = f(a) + f(b)$ for $(a,b) = 1$) and

$$f(n + 1) - f(n) < C_1$$

then $f(n) = c \log n + g(n)$ where $|g(n)| < C_2$.

This conjecture was recently proved by Wirsing. At the meeting in Oberwolfach this July Wirsing and I in this connection made the following conjecture. Assume

$$\overline{\lim_{p,\alpha}} f(p^\alpha) / \log p^\alpha = \infty .$$

Is it then true that

$$\overline{\lim_{n=\infty}} \frac{f(n + 1) - f(n)}{\log n} = \infty \ ?$$

or perhaps even

$$\overline{\lim_{n=\infty}} f(n+1)/f(n) = \infty \quad ?$$

For simplicity perhaps one can at first assume $f(p^{\alpha}) = f(p)$ or $f(p^{\alpha}) = \alpha f(p)$.

E. Wirsing, A characterization of log n as an additive arithmetic function, Institute Nat. di alta Mat. Vol IV 1970 45-57.