Paul Erdös

Problems and results in combinatorial number theory

Astérisque, tome 24-25 (1975), p. 295-310

<http://www.numdam.org/item?id=AST_1975__24-25__295_0>
I discuss a few problems and results, mostly connected with van der Waerden's theorem, which have occupied me and many of my co-workers a great deal over the last few years. I will try to give as complete references as possible, but of course I do not claim completeness and I apologise in advance for any omissions. In general I shall give references at the end of each chapter, but first I would like to call the readers attention to the interesting paper of van der Waerden: "How the proof of Baudet's conjecture was found", Studies in pure mathematics, papers in combinatorial theory, analysis... presented to Richard Rado, p. 251-260, London and New-York, Academic Press, 1971. A Brauer, by the way, states that the conjecture was really stated first by I. Schur. Recently a very short proof of van der Waerden's theorem was published by R. L. Graham and Bruce Rothschild (Proc. Amer. Math. Soc. 42 (1974), 385-386).

I introduce the following notations: A sequence of integers is said to have the property A(k) if it contains an arithmetic progression of k terms. It has the
property \( A(\omega) \) if it has the property \( A(k) \) for every \( k \). Van der Waerden's theorem can thus be expressed as follows: if we split the integers into \( t \) classes, then at least one class has the property \( A(\omega) \). A set of real numbers is said to have the property \( A(\mathbb{N}_0) \) if it contains an infinite arithmetic progression.

I have published several papers in number theory. Here, I only quote two recent ones, both of which contain many references: "Résultats et problèmes en théorie des nombres", Sém. Delange-Pisot-Poitou, 1972/73, n° 24 and "Problems and results in combinatorial number theory", A survey of combinatorial theory, 1973, North Holland, p. 117-138.

I. - The finite form of van der Waerden's theorem states: to every \( k \) and \( t \) there is an \( f(k,t) \) so that if we split the integers not exceeding \( f(k,t) \) into \( t \) classes, then at least one class has the property \( A(k) \).

Van der Waerden's proof gives a very bad estimate for \( f(k,t) \), (even for \( t = 2 \)) and this was one of the reasons which led Turán and myself to propose, more than forty years ago, the following problem, the positive solution of which of course implies van der Waerden's theorem:

Is it true that for every \( \varepsilon > 0 \) and integer \( k \) there is an \( n_0 = n_0(\varepsilon, k) \) so that every sequence \( 1 < a_1 < \ldots < a_s \leq n, \ n \geq n_0, \ s > \varepsilon n \) has the property \( A(k) \)? More precisely, denote by \( r_k(n) \) the smallest integer \( s \) for which every sequence \( 1 \leq a_1 < \ldots < a_s \leq n, \ s = r_k(n) \) has the property \( A(k) \). We conjectured that for every \( k \)

\[
(1) \quad r_k(n) = o(n).
\]

It is almost immediate that \( r_k(a+b) \leq r_k(a) + r_k(b) \) and this subadditivity implies that \( \lim_{n \to \infty} r_k(n)/n = c_k \) exists, but the proof of (1) seemed to present
great difficulties.

Originally we thought that in fact \( r_3(n) < n^{1-c} \), but this was disproved by Salem and Spencer who showed in 1942 that

\[
r_3(n) > n^{1-c/\log \log n}
\]

In 1946, F. Behrend showed:

\[
r_3(n) > n \exp(-c\sqrt{\log n})
\]

and this is still the best known lower bound for \( r_3(n) \).

In 1951, K. F. Roth proved that \( r_3(n) = o(n) \). More precisely he showed

\[
r_3(n) < cn / \log \log n
\]

and this upper bound has never been improved. The gap between (2) and (3) is very large and it would be desirable to obtain better bounds for \( r_3(n) \).

In 1967, Szemerédi proved that \( r_4(n) = o(n) \), his proof, which is a masterpiece of combinatorial reasoning, is completely elementary but very complicated and utilises van der Waerden's theorem. K. F. Roth using his method succeeded in eliminating the use of van der Waerden's theorem.

Very recently Szemerédi proved (1) in full generality. His proof, which will appear very soon in Acta Arithmetica is, needless to say, again a masterpiece of combinatorial ingenuity. Unfortunately he again used van der Waerden's theorem, but he believes that by the method of Roth it will be possible to eliminate the use of van der Waerden's theorem and thus perhaps obtain a weak, but not entirely ridiculous, upper bound for \( f(k, t) \).

The best known lower bounds for \( f(2, t) \) are due to Berlekamp who, improving previous results of Rado and myself and Schmidt, proved that

\[
f(2, t) > t 2^t
\]
if \( \ell \) is a prime number. It would be interesting to decide if

\[
\lim_{\ell \to \infty} \frac{f(2, \ell)}{\ell} = \infty
\]

is true. My guess would be that (4) is true.

In connection with (4) the following might be of use and interest. Denote by \( f(\varepsilon, 2, \ell) \) the smallest integer so that if one splits the integers not exceeding \( f(\varepsilon, 2, \ell) \) into two classes there is always an arithmetic progression of \( \ell \) terms which contains at least \( \frac{\ell}{2}(1+\varepsilon) \) terms of the same class. Clearly \( f(1, 2, \ell) = f(2, \ell) \).

It is possible that

\[
f(\varepsilon, 2, \ell) < c\varepsilon^\ell
\]

holds for some \( \varepsilon > 0 \), but I never succeeded in making any progress with (5). By the probabilistic method it is quite easy to show that

\[
f(\varepsilon, 2, \ell) > (1+c\varepsilon)^\ell,
\]

(P. Erdős, Math. Lapok 14, 29-37, in Hungarian).

Szemerédi's proof of (1) is very ingenious, but rather complicated. One of its basic tools is a lemma on the structure of bipartite graphs which I state here without proof. First I need some notation. Let \( A \) and \( B \) be disjoint sets, \( |A| = m, |B| = n \). Let \( G \) be a bipartite graph whose white vertices are \( A \) and black vertices \( B \). If \( X \subseteq A, Y \subseteq B \), then \( [X, Y] \) denotes the set of edges \((x, y)\) of \( G \) with \( x \in X, y \in Y \). Put \( \beta(X, Y) = |[X, Y]| \cdot |X|^{-1} \cdot |Y|^{-1} \) (i.e. \( \beta(X, Y) \) is the density of edges of our bipartite graph). \( G(u) \) denotes the set of vertices joined to the vertex \( u \).

Now we are ready to state the lemma of Szemerédi: to every \( \varepsilon_1, \varepsilon_2, \delta, \rho, \sigma \) there are \( m_0, n_0, M, N \) so that for every \( G \) for which \( |A| = m > M, |B| = n > N \), there are disjoint sets \( C_i \subseteq A, 1 \leq i \leq m_0 \) and \( C_{i,j} \subseteq B, 1 \leq j \leq n_0 \) which satisfy for every \( 1 \leq i \leq m_0 \),
Further we have for every $1 \leq i \leq m_0$, $1 \leq j \leq n_0$ and $S \subseteq C_i$, $T \subseteq C_i,j$ satisfying

$$|S| > \varepsilon_1 |C_i|, \quad |T| > \varepsilon_2 |C_i,j|$$

$$\beta(S, T) \geq \beta(C_i - C_i,j) - \delta .$$

Finally for every $1 \leq i \leq m_0$, $1 \leq j \leq n_0$, $X \subseteq C_i$

$$|G(X) \cap C_{i,j}| \leq (\beta(C_i, C_i,j) + \delta) |C_i,j| .$$

Szemerédi believes that the lemma is not best possible but can be sharpened in various ways. So far, however, there has been no success in this direction. The proof of the lemma is not as complicated as one could have expected.

There is no doubt that this deep lemma will have many applications. Here I only state a very recent theorem of Szemerédi. Denote by $G_r(n; m)$ a hypergraph of $n$ vertices and $m$ edges (i.e. $r$-tuples). Let $f_r(n; k, \ell)$ be the smallest integer so that every

$$G_r(n; f_r(n; k, \ell))$$

(i.e. every hypergraph of $n$ vertices and $f_r(n; k, \ell)$ $r$-tuples) contains a

$G_r(k; \ell)$ as a subgraph. V. T. Sos, W. Brown and I conjectured

$$f_3(n; 6, 3) = o(n^2) .$$

Szemerédi recently proved (7) using his lemma. We in fact thought that

$$f_3(n; 6, 3) < n^{2-c}$$

also holds, but Ruzsa disproved this by showing

$$f_3(n; 6, 3) > c n r_3(n) .$$

More generally it is probable that

$$f_3(n; k, k-3) = o(n^2) .$$
holds for every $k$, but Szemerédi's method does not seem to work for $k > 6$.

Perhaps

$$c_1 n r_{k-3}(n) < f_3(n; k, k-3) < c_2 n r_{k-3}(n)$$

holds for every $k \geq 6$. Ruzsa proved the lower bound in (8) for $k = 6, 7$ and 8, but the proof seems to run into difficulties for larger $k$. The work of Szemerédi and Ruzsa is not yet published.

It seems certain that Szemerédi's lemma will lead to further surprising insights.

---

REFERENCES


II. - A well known conjecture states that the primes have the property 
\( A(\infty) \). If I remember correctly it is known that they have the property \( A(16) \) and no doubt one could improve this, but as far as I can see the only way of proving the general conjecture would be to show that for \( n > n_k \) \( r_k(n) < \pi(n) \). In fact, perhaps for every \( k \) and \( t \) it is true that

\[
\lim_{n \to \infty} \frac{r_k(n)}{\log n} = 0.
\]

The following conjecture seems attractive to me: every sequence

\[ 1 \leq a_1 < \ldots \] satisfying \( \sum_{i=1}^{\infty} a_i^{-1} = \infty \) has the property \( A(\infty) \). I offer 2500 dollars for the proof or disproof of this conjecture. At the moment I see no hope for a proof but perhaps a counterexample can be constructed and this might be a relatively easy way of earning 2500 dollars, but I hope that the conjecture and (1) are both true.

In some cases in the past I proved theorems on primes where I used relatively few special properties of the primes and the fact that \( \pi(x) \) is large. In fact

I proved more than 35 years ago that for every \( r \) there are integers

\[ n_1(r), n_2(r), n_3(r) \] so that the equations

\[ n_1(r) = p + q, \quad n_2(r) = p - q, \quad n_3(r) = (p-1)(q-1) \]

have at least \( r \) solutions in primes \( p \) and \( q \). There seems little doubt though that the problem of \( k \)-tuples of primes in an arithmetic progression is much deeper.
Is it true that for every \( k \) there are \( k \) consecutive primes in an arithmetic progression? This problem seems completely unattackable to me, even for \( k = 3 \), though Renyi and I have some preliminary results for this case.

Before ending this chapter I state a few related problems and results.

Let \( a_1 < \ldots \) be an infinite sequence of integers and assume that no \( a_i \) is the distinct sum of other \( a \)'s, I proved that \( \sum a_i^{-1} < 103 \) (math. Lapok 13 (1962), 28-38, in Hungarian. An English version will appear in our joint paper with Benkoski in Math. of Computation). I heard at the last meeting of the Amer. Soc. (April 1974) that 103 can in fact be replaced by 5, but that the result does not hold with 2.

Unfortunately I do not remember who proved these results. It was also suggested that the maximum of \( \sum a_i^{-1} \) is probably not much greater than 2. In February 1973, I conjectured that if \( a_1 < a_2 < \ldots < a_n \) is such that all the sums \( \sum_{i=1}^{n} \epsilon_i a_i \), \( \epsilon_i = 0 \) or 1 are all distinct, then:

\[
\max_{i=1}^{n} \sum a_i^{-1} = 2^{-1-n}
\]

and the maximum is attained if and only if \( a_i = 2^{i-1} \). Ryavec found a simple analytic proof and recently E. and G. Szekeres found an elementary proof. Here I may mention one of my oldest conjectures: Let \( a_1 < \ldots < a_n \leq X \) be such that all the sums \( \sum_{i=1}^{n} \epsilon_i a_i \) are distinct; is it true that

\[
n < \frac{\log X}{\log 2} + C?
\]

Moser and I proved that

\[
n < \frac{\log X}{\log 2} + \frac{\log \log X}{2 \log 2} + C.
\]

Let \( a_1 < a_2 < \ldots \) be an infinite sequence of integers; assume that for \( i \leq j < k \), \( a_j + a_k \not\equiv 0 \pmod{a_i} \). Put \( A(X) = \sum_{a_i < X} 1 \), Sarközi and I proved \( A(X) = o(X) \), we conjecture that \( \sum a_i^{-1} \) and that \( A(X) < X^{1-\epsilon} \) for infinitely many \( X \). There is an interesting finite problem here which causes unexpected difficulties:
Let $a_1 < \ldots < a_n < X$ and assume that for $i < j < r$ $a_j + a_r \neq 0 \pmod{a_i}$, then $n \leq \lfloor \frac{X}{3} \rfloor + 1$. The $n+1$ integers $2n$, $2n+1$, $\ldots$, $3n$ show that our conjecture, if true, is best possible. The proof presents difficulties which we have not been able to overcome. If we assume $a_r + a_s \neq 0 \pmod{a_k}$ (i.e. without $k < r < s$), then $n = o(X)$ follows from $r_3(X) = o(X)$, since the $a$'s cannot contain a three term arithmetic progression. Szemerédi proved that $n \leq \lfloor \frac{X}{3} \rfloor + 1$ if $(a_r + a_s)/a_k$ can never be an integer different from 2.

---

**REFERENCES**


P. ERDÖS and A. RENYI. - Some problems and results on consecutive primes. Simon Stevin 27 (1950), 115-126.

P. ERDÖS. - Problems and results in additive number theory. Colloque sur la théorie des nombres, Bruxelles, George Thone, Liège, Masson et Cie, Paris, (1955), 127-137. (Our proof with Moser is at the end of this paper).


---

III. - Some infinite problems. It is clear that one can give a sequence of integers which tends to infinity as fast as one likes and whose complement does not have the property $A(N)$. This follows from the fact that the number of arith-
metric progressions is denumerable. I then asked: "Can one decompose the reals into two sets \( S_1 \) and \( S_2 \) so that \( S_1 \) does not have the property \( A(3) \) and \( S_2 \) does not have the property \( A(\aleph_0) \)?" Davies proved the existence of such a decomposition using \( 2^\aleph_0 = \aleph_1 \), but recently Baumgartner gave an example of such a decomposition without using any hypothesis. Baumgartner's paper on the subject will be published soon.

The following more general question can now be asked. Let \( k \) be a given integer. Can one decompose the set of real numbers into countably many sets \( S_t, \ t = 1, 2, \ldots, \) such that every \( S_t \) intersects every \( k \)-term arithmetic progression in at most two terms but the complement \( \bar{S}_t \) of \( S_t \) never has the property \( A(\aleph_0) \)?

It seems that Baumgartner's method will give the existence of these sets.

(Added in proof: Baumgartner has shown the existence of these sets).

I hope that one can ask more general and non-trivial questions of the following type. Consider a family \( F \) of denumerable sets \( \{A_\alpha\} = a_1^{(\alpha)} < \ldots \) of real numbers. We say that \( F \) has the property \( P_3 \) if there is a set which intersects each \( A_\alpha \in F \) but never contains three consecutive elements \( \{a_1^{(\alpha)}, a_{i+1}^{(\alpha)}, a_{i+2}^{(\alpha)}\} \) of any \( A_\alpha \). Baumgartner's theorem states that the family of all infinite arithmetic progressions has the property \( P_3 \). Assume that the family \( F \) is such that if \( a_1 = a_j \) and \( a_{i+1} = a_{j+1} \), then for every \( t > 0 \), \( a_{i+t} = a_{j+t} \), (the infinite arithmetical progressions certainly have this property). Is it true that \( F \) has the property \( P_3 \)? Assume now that every countable sub-family of \( F \) has the property \( P_3 \). Does it follow that \( F \) has the property \( P_3 \)? I would guess that the answer is no. I apologise if one (or both) of these questions has a trivial negative answer, they were only formulated recently.
Hindman recently proved the following conjecture of Graham and Rothschild: Split the integers into two classes in an arbitrary way. Then there always is an infinite subsequence \( a_1 < a_2 < \ldots \) so that all the sums \( \sum \varepsilon_i a_i, \varepsilon_i = 0 \) or 1 are in the same class. Recently Baumgartner found a simple proof of Hindman's theorem. The results stated in this chapter are not yet published.

I have tried to formulate a conjecture which would be in the same relation to Hindman's theorem as Szemerédi's theorem is to van der Waerdens. I have not been very successful so far. Perhaps the following result holds. Let \( a_1 < a_2 < \ldots \) be a sequence of integers with positive upper density. Then there is an integer \( t \) and an infinite subsequence \( a_1 < a_2 < \ldots \) so that all the sums \( a_i + a_j + t \) are again \( a \)'s.

In a previous paper I stated the following problem: Split the real numbers into two classes. Does there exist a set \( \{a_\alpha\} \), \( 1 \leq \alpha < \omega_1 \) of power \( \mathfrak{N}_1 \) so that all the sums

\[
a_{a_1} + a_{a_2}, \quad 1 \leq a_1 < a_2 < \omega_1
\]

belong to the same class? I stated that I cannot settle this question even if the continuum hypothesis is assumed. Some time ago I noticed that using the methods of our paper with Hajnal and Rado I can prove -assuming the continuum hypothesis- that the set of reals can be split into two disjoint classes \( S_1 \) and \( S_2 \) so that if \( A, B \) with \( |A| = \mathfrak{N}_1 \), \( |B| = \mathfrak{N}_0 \) are any two sets of reals there always are real numbers \( X_1 \in S_1 \), \( Y_1, Y_2 \in S_2 \), \( X_2 \in S_2 \) so \( X_1 + Y_1 \in S_1 \), \( X_2 + Y_2 \in S_2 \).
IV. - In the last chapter we discuss miscellaneous problems on arithmetic progressions and related topics.

(i) Is it true that for every $k$ and $r$ there is a sequence without the property $A(k+1)$, but is such that if we split it into $r$ subsequences at least one of them has the property $A(k)$? (added in proof: Spencer has recently shown that such a sequence exists).

The conjecture was motivated by the following older conjecture of Hajnal and myself: Is it true that for every $\ell$ and $r$ there is a graph not containing a $K(\ell+1)$ (i.e. a complete graph of $\ell+1$ vertices) but if one colours its vertices by $r$ colours, then at least one colour contains a $K(\ell)$? J. Folkman proved the existence of such a graph for $r=2$ and every $\ell$ (he probably had a proof for $r=4$). Recently the problem was settled in full generality by Nesetril an Rödl (their paper is not yet published).

(ii) Riddell defines $g_k(n)$ as the largest integer so that every sequence $a_1 < \ldots < a_n$ contains a subsequence of $g_k(n)$ terms not having the property $A(k)$. One woulds guess at first that $g_k(n) = r_k(n) - 1$, but Riddell shows that this is not always true. He also obtained some lower bounds for $g_k(n)$ which Riddell and I
slightly improved. This was succeeded by a general result of Komlos, Subjok and Szemerédi (their paper will be published soon). They obtain \( g_k(n) > c r_k(n) \) as a special case of their theorem. It is unknown if \( g_k(n) < r_k(n) - 1 \) holds for infinitely many values of \( n \), or if for every \( k \)

\[
\lim_{n \to \infty} \frac{g_k(n)}{r_k(n)} = 1.
\]

J. Riddel, on sets of numbers containing no \( t \) terms in arithmetic progression, Nieuw Archief voor Wiskunde 17, 204-209.

(iii) Let \( r_k^{(t)}(n) (k \leq t) \) be the smallest integer so that every sequence

\[ 1 \leq a_1 < \ldots < a_s \leq n, \quad s = r_k^{(t)}(n) \]

contains at least \( k \) terms of an arithmetic progression of length \( t \). Clearly \( r_k^{(k)}(n) = r_k(n) \). Using Behrend's idea one easily obtains for every \( k > 2 \)

\[
r_k^{(t)}(n) < c \exp\left( -\left( \log n \right)^{\alpha(k, t)} \right).
\]

Szemerédi and I conjectured that for \( 3 \leq k_1 \leq k_2, \quad t_2/k_2 \geq t_1/k_1 \)

\[
\lim_{n \to \infty} \frac{r_{k_2}^{(t_2)}(n)}{r_{k_1}^{(t_1)}(n)} = \infty
\]

unless \( k_1 = k_2 \) and \( t_1 = t_2 \). Even if (1) is proved open problems remain, e.g. what is the value of

\[
\lim_{n \to \infty} \frac{r_3(n)}{r_4^{(5)}(n)}?
\]

(iv) Denote by \( f(n; k, t) \) \( k < t \) the smallest integer with the property that if the sequence \( a_1, \ldots, a_n \) contains \( f(n; k, t) \) \( k \) term arithmetic progressions then it contains an \( t \)-term arithmetic progression. I conjecture that
f(n; k, t) = o(n^2) and perhaps f(n; k, t) < n^{2-\varepsilon(k, t)}. I have not even been able to prove that f(n; 3, 4) = o(n^2).

More generally let f(n; k_1, t_1, k_2, t_2) be the smallest integer with the following property: Let A_n be any sequence of n distinct real numbers. Assume that there are f(n; k_1, t_1, k_2, t_2) arithmetic progressions of t_1 terms which intersect A_n in at least k_1 terms, then there is an arithmetic progression of t_2 terms which intersects A_n in at least k_2 terms. I hope that some interesting results can be found about f(n; k_1, t_1, k_2, t_2).

Perhaps if A_n contains c_1n^2 arithmetic progressions of three terms, then it must contain an arithmetic progression of c_2\log n terms (c_2 = c_1(c_1)). By probabilistic methods it is easy to see that, if true, this is best possible, apart from the value of c_2.

Denote by g(n, k, c) the largest integer so that every sequence
\[
1 \leq a_1 < \ldots < a_s \leq n, \ s \geq c n, \ contains \ at \ least \ g(n, k, c) \ arithmetic \ progressions
\]
of k terms. Varnavides proved g(n, k, c) > \alpha_k(c)n^{2} for k = 3 and this was extended to all k by Szemerédi. A good estimation of \alpha_k(c) as c \to \infty does not seem easy and I cannot prove that
\[
\lim_{c \to \infty} \lim_{n \to \infty} \frac{g(n, k_1, c)}{g(n, k_2, c)} = 0 \ \text{for} \ k_1 > k_2.
\]


(v) Is it true that if f(n) = \pm 1 is any function defined on the integers, then to every c there is a d and an m so that
\[
\sum_{k=1}^{m} |f(kd)| > c?
\]
COMBINATORIAL NUMBER THEORY

This is one of my oldest conjectures (about 40 years old) and I offer 300 dollars for a proof or disproof. Perhaps (1) remains true if \( f(n) \) is complex valued and \( |f(n)| = 1 \), or perhaps it could be true in more general vector spaces.

If \( f(n) = \pm 1 \) and \( f(n) \) is assumed to be multiplicative we obtain the conjecture that \( |\sum_{k=1}^{n} f(k)| \) cannot be bounded. For a more general conjecture see N. G. Tchudakoff, Theory of the characters of number semigroups, International Coll. Zeta function, Bombay 1956, 11-16.

The sharpest quantitative form of (1) which could be true states as follows. There is an absolute constant \( c_1 \) so that if \( f(n) = \pm 1, \ n = 1, 2, \ldots \) there always are integers \( d \) and \( m \) so that \( md < x \) and

\[
\left| \sum_{k=1}^{m} f(kd) \right| > c_1 \log x .
\]

(vi) Several years ago I asked the following question. Let \( a_1 < \ldots < a_n \leq X \) be a sequence of integers. Assume that no \( a \) divides the sum of the other \( a \)'s. Put \( \max n = F(X) \). I thought that \( F(X) \) was less than a power of \( \log X \), but E. Straus proved that

\[
F(X) > \exp \left( 1 + o(1) \right) \sqrt{\frac{2 \log X}{\log 2}} .
\]

What is more interesting, Straus observed that the problem is essentially equivalent to the following much more interesting one. Let \( 1 \leq a_1 < \ldots < a_m \leq X \) be a sequence of integers such that no \( a \) is the arithmetic mean of any other \( a \)'s. Put \( \max m = f(X) \). Determine or estimate \( f(X) \). Straus, in fact, proved that (1) holds for \( f(X) \) and Straus and I proved \( f(X) < c^{3/4} \). Szemerédi recently somewhat improved the exponent \( 3/4 \), but it seems probable that \( f(X) = o(X^{\epsilon}) \) and we are very far from being able to prove this.
REFERENCES


---

Paul ERDÖS
Universités du Monde