SOME NEW PROBLEMS AND RESULTS IN NUMBER THEORY

Paul Erdös

+*+*+

Introduction

As I already stated several times, I published many papers by the same or similar titles during my long mathematical life. Here I refer only to three of them. All three of them contain many solved and unsolved problems and many references. I try to avoid duplication as much as possible and will state older problems only if they are not easily accessible, or not stated quite correctly, or if some progress has been made towards their solution. I will include proofs only rarely. It happens surprisingly often that one has difficulties in reconstructing proofs, when I only write 'it follows easily' - and in some cases the reason for the difficulty was that the 'proof' was wrong or at least not quite correct. Whenever possible I will try to give an indication of the proof.

P. Erdös and R.L. Graham, Old and new problems and results in combinatorial number theory, Monographie No. 28, de L'Enseignement Math., 1980. This paper contains about 200 references. We will refer to it as I.

P. Erdös, On many old and some new problems of mine in number theory, Congress Num. Vol. 30, Winnipeg, Canada (Utilitas

Math.), Proc. Tenth Conf. in Combinatories, 1980, 3-27. I refer to this paper as II. This paper is not easily accessible.

P.Erdös, Problems and results on combinatorial number theory III, Number Theory Day, Springer - Lecture Notes 626 (1976), 43-73.

§ 1

I will start with some problems on additive number theory.

1. About 50 years ago Sidon called a sequence of integers $1 \leq a_1 < a_2 < \dots$, a B_2 sequence if the sums $a_1 + a_j$ are all distinct. He asked for a B_2 sequence for which a_k increases as slowly as possible. He was led to this question by the study of lacunary trigonometric sequences. He easily constructed a B_2 sequence with $a_k < k^4$ for all k. I showed without difficulty that the greedy algorithm gives $a_k < k^3$ and Sidon and I both thought that for every $\varepsilon > 0$ there is a B_2 sequence for which for every $k > k_0(\varepsilon)$, $a_k < k^{2+\varepsilon}$ holds.

We could not even prove that there is a B_2 sequence for which

$$a_k / k^3 \longrightarrow 0. \tag{1}$$

This modest conjecture remained open until very recently and was proved by a very ingenious new method by Ajtai, Komlos and Szemeredi.

The following problem is perhaps of interest here. Is there an infinite sequence satisfying (1) for which $n = a_1 - a_j$

has a unique solution ? The method of Ajtai, Komlos and Szemeridi does not seem to work here. The greedy algorithm again gives such a sequence satisfying $a_k < ck^3$.

Let $a_1 < a_2 < \dots$ be a B_2 sequence. I proved

$$(2) \qquad \sum_{a_k < x} \frac{1}{a_k^{1/2}} = o(\log x).$$

In fact my proof gives $< c(\log x)^{1/2}$. Put

$$f(x) = \max \sum_{a_k < x} \frac{1}{a_k^{1/2}} ,$$

where the maximum is taken over all B_2 sequences. I proved that $f(x) \longrightarrow \infty$, but I have no good upper or lower bounds for $f(x)$.

For further problems and results on B_2 sequences see H. Halberstam and K. F. Roth, Sequences, Oxford University Press 1966 and A. Stohr, Geloste und ungeloste Fragen uber Prasen der naturlichen Zahlenreihe II., J. reine angew. Math. 194 (1955), 111-190. The proof of (2) and $f(x) < c(\log x)^{1/2}$ is substantially contained on p. 89-90 of the book of Halberstam and Roth.

M. Ajtai, J. Komlos and E. Szemeredi, On dense infinite Sidon sequences, European J. Combinatorics, 2 (1981), 1-11.

P. Erdös, Some applications of Ramsey's theorem to additive number theory, European J. Combinatorics, 1 (1980), 43-46.

2. Consider the set of all solutions of

$$(1) \qquad n = a_1 + a_2 + \dots \quad , a_1 < a_2 < \dots .$$

In other words we consider the set of all partitions of n into distinct integers. Denote by $f(n)$ the smallest integer for which if we split the integers into $f(n)$ classes (1) has a solution in integers all of which are in the same class. In the language of hypergraphs $f(n)$ is the chromatic number of the non-uniform hypergraph whose vertices are the integers and whose edges are the solutions of (1). I proved several years ago that $f(n) \longrightarrow \infty$ and that in fact $f(n) > c_1 n^{\alpha}$. The exact determination of $f(n)$ does not seem to be easy.

Recently Spencer proved that $f(n) \longrightarrow \infty$ for a very small subclass of the solutions of (1) and proved many interesting related questions and raised interesting new questions.

My proof of $f(n) \longrightarrow \infty$ is based on the following

Lemma. To every $\varepsilon > 0$ there is a k so that every set of $\frac{\varepsilon n}{k \log n}$ set of primes $> \frac{n}{k}$ contains a solution of (1) (if $n > n_0(\varepsilon, k)$).

The proof of the Lemma follows easily by using the ideas of Schnirelman and Brun - I do not give the details.

The Lemma immediately implies $f(n) \to \infty$ and by a slight sharpening one can deduce $f(n) > c\, n^{\alpha}$, but I do not see how to determine the best value of α.

In the language of hypergraphs my proof works as follows: We find a set of m vertices (the primes $< \frac{n}{k}$) for which the largest independent set has size $< \varepsilon . m$ (i.e. its stability number is $< \varepsilon . m$).

Let $A = \{a_1 < a_2 < \dots\}$ be an infinite sequence of integers; denote by $A^{(\infty)}$ the set of integers which are the distinct sum of the a's. I proved that if $\bigcup_{i=1}^{k} A_i$ is the set of all integers then for at least one i, $A_i^{(\infty)}$ has upper density 1 and upper logarithmic density $\geq \frac{1}{2}$. The proof again uses our Lemma, the details will not be given. I am not quite sure if $\frac{1}{2}$ is best possible here but it is easy to see that it can not be $> \frac{3}{4}$. To see this let $n_{i+1} = n_i^4$ and A_1 be the set of integers x such that $n_{2i} \leq x < n_{2i+1}$, $i = 1,2,\dots$, and A_2 be the complement of A_1.

The upper logarithmic density of $a_1 < a_2 < \dots$ is defined as

$$\limsup \frac{1}{\log x} \sum_{a_i < x} \frac{1}{a_i} .$$

J. Spencer, Sure sums, Combinatorica 1 (1981), 203-208.

3. Let $1 \leqslant a_1 < \dots < a_k \leqslant n$ be a sequence of integers. Assume that all the sums $a_1 + a_j$ are distinct. An old theorem of Turán and myself then states that

$$\max k = (1 + o(1))\, n^{1/2} \tag{1}$$

and an old conjecture of ours states that in fact

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

I offer 500 dollars for a proof or disproof of (2).

Assume now only that the number of distinct sums of the form $a_1 + a_j$ is $(1+o(1)) \binom{k}{2}$. I recently observed that this weaker assumption no longer implies (1) and in fact I have an example with $k \geqslant \frac{2n^{1/2}}{3^{1/2}}$. Note $k \leqslant (1 + o(1))\,(2n)^{1/2}$ is trivial and I believe $\max k < c\, n^{1/2}$ for some $c < 2^{1/2}$, but I have not been able to prove this.

P. Erdös and P. Turán, On a problem of Sidon in additive number theory and some related questions, J. London. Math. Soc. 16 (1941), 212-215.

4. An old conjecture of mine states that if $f(n)$ is the least integer not of the form $a + b$ where $P(a,b) \leqslant n$ then for every k and $n > n_0(k)$ we have $f(n) > n^k$ ($P(m)$ is the greatest prime factor of m). This conjecture does not look hard but I could not get anywnere with it.

Let $h(n)$ be the smallest integer not of the form

$$(1) \quad a_1 + a_2 + \dots + a_r \quad \text{where} \quad P(a_1 \dots a_r) \le n, \ (a_i, a_j) = 1, \quad 1 \le i < j \le r.$$

In (1) r is arbitrary but $(a_i, a_j) = 1$ implies $r = \pi(n)$. Recently I proved that

$$e^{c_1 n} < h(n) < e^{c_2 n} .$$

Probably there is a c for which

$$(2) \qquad h(n) = \exp((1+o(1))c \cdot n),$$

but I have not been able to prove (2).

5. Let $1 = a_1 < a_2 < \dots$ be an infinite sequence of integers for which no a is the sum of consecutive a's , i.e.

$$(1) \qquad a_r \ne a_i + a_{i+1} + \dots + a_j \quad \text{for all} \quad i < j < r .$$

On p.94 of I, the following question is stated: Let A satisfy (1). Does it follow that the density of A must be 0 ?

Here my normally good memory failed badly. On p.20 of II I state: Harzheim and I considered the following problem. Let A satisfy (1). Is it true that the upper density of A is $\frac{1}{2}$? We give the following simple construction to show that the upper density can be $\frac{1}{2}$. Suppose $1 \le a_1 < \dots < a_k$ is already defined.

Then $a_{k+1} = a_k^4$, $a_{k+2} = a_k^4 + a_k^2$, $a_{k+2+i} = a_k^4 + a_k^2 + i$, $1 \leq i \leq a_k^4 - a_k^2$. Clearly this sequence satisfies (1) and has upper density $\frac{1}{2}$.

I have to apologise that I forgot Harzheim in I and that I forgot what is in II. The following questions might be of interest. Let A satisfy (1). Is the logarithmic density of A zero.? Is it true that

$$A(x) = \sum_{a_i < x} 1 \leqslant \frac{x}{2} + O(1)? \ .$$

put

$$f(x) = \max \sum_{a_i < x} \frac{1}{a_i} \ ,$$

where the maximum is taken over all sequences satisfying (1). Determine or estimate $f(x)$ as well as possible. Harzheim and I obtain $f(x) \gg \log \log x$. Is it true that $f(x)/\log \log x \to \infty$?

6. On p.50 of I we ask: Let $A = \{a_1 < \dots \}$, $B = \{b_1 < \dots . \}$ be two sequences of integers satisfying $A(x) > c\,x^{1/2}$, $B(x) > c\,x^{1/2}$. Is it true that $a_i - a_j = b_k - b_\ell$ has infinitely many solutions ? R.Freud pointed it out to us that the answer is obviously no ! The a's are the integers of the form $\Sigma \ \varepsilon_i 2^{2i}$ and the b's $\Sigma \ \varepsilon_i 2^{2i+1}$, $\varepsilon_i = 0$ or 1.

In this case

$$(1) \qquad \liminf \frac{A(x)\ B(x)}{x} = 1, \ \limsup \frac{A(x)\ B(x)}{x} = 3/2 \, .$$

and

$$(2) \qquad \min\,(A(x),\ B(x)) \geq (1 + o(1))\ \left(\frac{x}{2}\right)^{1/2} .$$

Trivially

$$(3) \qquad \limsup \frac{A(x)\ B(x)}{x} \leqslant 2$$

and Freud and I showed that (3) is best possible. Probably

$$\liminf \frac{A(x)\ B(x)}{x} \leqslant 1.$$

Several further problems remain which we hope to investigate.

Now I discuss some problems on prime numbers.

1. Let $p_1 < \ldots$ be the sequence of consecutive primes. Observe that the numbers $k! + 2, \ldots, k! + k$ are all composite Thus $\limsup p_{n+1} - p_n = \infty$. This idea gives that for infinitely many n

$$(1) \qquad p_{n+1} - p_n > c \cdot \frac{\log n}{\log \log n} .$$

Put

$$L_n = \frac{\log n \log \log n \ \log \log \log \log n}{(\log \log \log n)^2} .$$

The sharpest improvement known at present of (1) gives that for infinitely many n and for some $c > 0$

$$(2) \qquad p_{n+1} - p_n > c\, L_n .$$

This is due to Rankin.

Our powerlessness in dealing with prime number problems in shown by the fact that how little better (2) is than the trivial result (1). (2) has not been improved substantially for more than 40 years. The only progress was that Schonhage and Rankin improved the value of the constant c. I offered 10000 dollars for a proof that (2) holds for every value of c.

I proved that there is a constant c_1 so that for infinitely many n

$$(3) \qquad \min (p_{n+1} - p_n \, , \; p_n - p_{n-1}) > c_1 \cdot L_n$$

and I conjectured that there is a constant c_k so that for infinitely many n

$$(4) \qquad \min_{i = 1,2,\ldots k} (p_{n+k+1} - p_{n+i}) > c_k \, L_n \, .$$

Very recently Maier proved (4) for every k. Nevertheless I am sure that if

$$D_k(x) = \max_{p_n < x} \; \min_{i = 1,2,..k-1} (p_{n+i+1} - p_{n+i}),$$

then

$$(5) \qquad \lim_{x \longrightarrow \infty} D_{k+1}(x)/D_k(x) = 0$$

but I can not prove (5) even for $k = 1$. Cramer conjectured (using a plausible probabilistic argument) that

$$(6) \qquad \limsup_{x \longrightarrow \infty} D_1(x)/(\log x)^2 = 1.$$

Similarly one would expect that

$$(7) \qquad \limsup_{x \longrightarrow \infty} D_k(x)/(\log x)^{1+ \frac{1}{k}} = 1.$$

and this would of course imply (5). The proof of (6) and (7) can not be expected in the foreseeable future !

(5) can be posed for other sequences e.g. for the square-free numbers or for the integers of the form $x^2 + y^2$. I had no success in trying to prove (5) even for $k = 1$ for these sequences and again do not expect success in the foreseeable future.

More generally let $p_1 < p_2 < \dots$ be an infinite sequence of primes and $u_1 < u_2 < \dots$ is the sequence of integers not divisible by any of the p's. Perhaps one can obtain conditions which will imply that (5) is satisfied for the u's . I hope to investigate this question - if I live!

Let n be an integer $1 = a_1 < a_2 < \dots < a_{\varphi(n)} = n - 1$ are the integers relatively prime to n. Put

$$J(n) = \max (a_{k+1} - a_k). \tag{8}$$

J(n) is named after Jacobsthal who investigated this function. In a paper dedicated to Jacobsthal's 80th birthday, I proved that for almost all n ($\omega(n)$ is the number of distinct prime factors of n)

$$J(n) = (1 + o(1)) \omega(n) \cdot \frac{n}{\varphi(n)} . \tag{9}$$

Put $J(n) = J_1(n)$ and

$$J_r(n) = \max \min_{0 \leq i \leq r-1} (a_{k+i+1} - a_{k+i}).$$

I hope to investigate $J_r(n)$ in the near future - if there is a future for me! .

2. I proved that

$$\liminf_{n \to \infty} (p_{n+1} - p_n)/ \log n < 1. \tag{1}$$

The first really significant improvement of (1) was due to Bombieri and Davenport who proved that

$$\liminf_{n \to \infty} (p_{n+1} - p_n)/\log n < 0.455. \tag{2}$$

There is no doubt that the true value of the lim inf is 0 and in fact surely the number $\frac{p_{n+1} - p_n}{\log n}$ are everywhere dense in (o,∞), but nothing like this can be proved at present. Ricci and I proved that the set of limit points of $\frac{p_{n+1} - p_n}{\log n}$ form a set of positive measure, but there is no finite value α for which we can be sure that α belongs to our set.

I tried to prove that

$$\liminf_{n \to \infty} \max \{(p_{n+1} - p_n), (p_n - p_{n-1})\} / \log n < 1,$$

but to my unplesant surprise I was never successful. I was further never able to prove that there is an absolute constant $c < 1$ so that for every k

$$\liminf \frac{p_{n+k} - p_n}{k \log n} < c .$$

R.A.Rankin, The difference between consecutive prime numbers, J. London Math. Soc. 13 (1938), 242-247.

P.Erdös, The difference of consecutive primes, Duke Math. J. 6 (1940), 438-441 and Problems and results on the difference of consecutive primes, Publ. Math. Debrecen 1 (1949), 33-37.

G.Ricci, Rechenhes sur l'allure de $\frac{p_n \ -p_n}{\log p_n}$ coll sur la theorie des nombres Bruxelles 1955, 93-96, Sull undamento della differenze di numerie primi consecutive Riv. Math. Univ. Burma, 3(1959), 3-59. My proof appeared in 1955, in the lecture notes held at a number theory conference held at the Villa Borghere at Lake-Como.

E.Bombieri and H.Davenport, Small differences between prime numbers, Proc. Roy. Soc. Ser. A. 293 (1966), 1-18.

H.Maier, Chains of large gaps between consecutive primes, Advances in Math. 39 (1981), 257-269.

One could ask for the slowest growing function f(x) for which

$$\pi(x + f(x)) - \pi(x) = (1 + o(1) \frac{f(x)}{\log x} . \tag{1}$$

On probability grounds perhaps one could hope that if

$\frac{f(x)}{(\log x)^2} \longrightarrow \infty$ then (1) holds.

From below we immediately obtain that by Rankin's result that (1) can hold then we must have

$$\frac{f(x)}{L(x)} \longrightarrow \infty , \tag{2}$$

and it is not clear to me whether there is any prospect in the futube to improve (2).

For the study of the local distribution of the prime numbers the following function seemed useful:

$$F(n) = \sum_{p < n} \frac{1}{n-p} .$$

It is immediate from the prime number theorem that the mean value of $F(n)$ is 1. I claimed that I can prove that

$$(3) \qquad \frac{1}{x} \sum_{n=1}^{x} F^2(n) \longrightarrow 1.$$

(3) no doubt is true but Pomerance pointed it out to me that my proof only gives

$$(4) \qquad c_1 < \frac{1}{x} \sum_{n=1}^{x} F^2(n) < c_2 .$$

(4) follows easily from Brun's method.

It easily follows from the prime number theorem of Hoheisel that $F(n) > c$ for some positive absolute constant c and one can hope that

$$\lim\inf F(n) = 1, \quad \lim\sup F(n) = \infty$$

and perhaps $F(n) < c \log\log\log n$. As far as I know no proof of even $F(n) = o(\log\log n)$ is in sight. $F(n) < c \log\log n$ follows easily by Brun's method.

Let $1 < a_1 < \dots$ be an arbitrary sequence of integers satisfying $a_n = (1 + o(1))\, n \log n$. Put

$$F_1(n) = \sum_{a_k < n} \frac{1}{n - a_k} .$$

I conjectured that 1 is always a limit point of the sequence $F_1(n)$. Montgomery proved this; his proof is ingenious and not at all trivial.Ruzsa and I conjectured that 2 is also a limit point of $F_1(n)$, but Ruzsa pointed it out that for every $\alpha \neq 1$ and $\alpha \neq 2$ there is a seqence $a_n = (1 + o(1))\, n \log n$ for which α is not a limit point of $F_1(n)$.

One could perhaps study

$$\sum_{\substack{p < 2n \\ p \neq n}} \frac{1}{n-p} = \Sigma_1^{(n)} - \Sigma_2^{(n)} , \quad \Sigma_1^{(n)} = \sum_{p < n} \frac{1}{n-p} , \quad \Sigma_2^{(n)} = \sum_{n < p < 2n} \frac{1}{p - n} .$$

Probably this sum changes sign infinitely often and is in fact dense in $(-\infty, \infty)$. Perhaps

$$(5) \qquad \sum \frac{1}{n - p} \to 0 , \text{ where } p < 2n, \ |p-n| > (\log n)^2 .$$

(5) if true is of course hopeless. I did not yet have time to investigate whether and for which $f(n)$

$$\sum \frac{1}{n-p} , \quad p < 2n, \ |n - p| > f(n)$$

definitely does not tend to 0; perhaps $f(n)$ must be $o((\log n)^{1+\varepsilon})$ for every $\varepsilon > 0$.

Let again $a_n = (1 + o(1))\ n \log n$. Perhaps

$$\lim\ \sup \sum_{\substack{a_k \neq n \\ a_k < 2n}} \frac{1}{n - a_k} \geq 1 \text{ and } \lim\ \inf \sum_{\substack{a_k \neq n \\ a_k < 2n}} \frac{1}{n - a_k} \leq -1 .$$

I state some miscellaneous somewhat unconventional results and problems on prime numbers.

Straus and I conjectured that for all sufficiently large p_k there are indices i for which

$$(1) \qquad p_k^2 < p_{k+i}\ p_{k-i} \cdot$$

Pomerance showed that (1) fails for infinitely many k. Pomerance and I then conjectured that (1) holds for almost all k. i.e. the density of the indices k for which (1) does not hold is zero. This certainly must be true but so far we have not been a able to prove it. This will undoubtedly hold for much more general sequences than primes.

Pomerance and I conjectured that there is an absolute constant C so that the number of distinct multiples of the primes p, $n < p < 2n$ in any interval $(x, x + C\ n)$ is always g greater than $c_1\ n/\log n$. The constant C must be greater than 2 since otherwise consider the integers in $(m\ A_n \pm n)$ where A_n is the product of the primes in $(n,2n)$. Clearly only A_n is a multiple of a prime $n < p < 2n$ in this interval. We hope that our conjecture holds for every $c > 2$ but we can not even prove it if our interval has length n^{1+c} perhaps we overlook simple argument

3. Recently I conjectured that for $k > k_o$ the congruence

$$u \equiv p_i\ p_j \pmod{p_k},\ 1 \leq i < j < k$$

is solvable for every $u \not\equiv 0 \pmod{p_k}$. Sarkozy and Odlyzko proved using exponential sums and the generalised Riemann hypothesis that for every $u \not\equiv 0 \pmod p$ the congruence $p_i \cdot p_j \cdot p_\ell = u$ $\pmod p$, $i < j < \ell < k$ is solvable for $k > k_o$. Brun's method gives that the number of distinct residues $\pmod{p_k}$ of the form $p_i\ p_j$ is $> c\ p_k$.

I conjectured that 7 is the largest prime p_k for which the primes $p_k, p_{k+1}, \dots, p_{k+p_k-1}$ form a complete set of residues $\pmod{p_k}$. I thought that this conjecture will be very difficult, but I was wrong since Pomerance gave a simple proof of the conjecture for $k > k_o$. Here is the simple idea of his proof. The primes $(2\ell - 1)\ p_k < p_r < 2\ell\ p_k$ are congruent $\pmod{p_k}$ to an even number and the primes $2\ell p_k < p_r < (2\ell + 1) p_k$ are congruent to an odd number. From the sharp form of the prime number theorem it immediately follows that the first interval contains more primes than the second one for $\ell < \log k$ if $k > k_o$. Since the number of the even residues is the same as the number of off residues this immediately, implies my conjecture for $k > k_o$. I am sure that with a little more trohble one can prove my conjecture/ for all

$p_k > 7$. Pomerance proved with somewhat more trouble that if $n > n_o$ and $p_1 < \cdots < p_{\varphi(n)}$ is the sequence of consecutive primes which are not divisors of n then this sequence does not contain every residue a (mod n), $(a,n) = 1$.

Another old problem of mine states : Is it true that for every $p > 2$ there is a prime $q < p$ which is a primitive root of p? It is surprising that this question does not seem to be easy.

4. About 30 years ago I conjectured that for every odd $n > 105$ the integers

$$n - 2^k, \quad k \geq 1, \quad 2^k < n \tag{1}$$

can not all be primes. Vaughan proved that the number of integers $n < x$ for which the numbers (1) are all primes is rather small, but the proof of my conjecture is nowhere in sight.

On the other hand Van der Corput and I proved that for infinitely many odd n the numbers (1) are never primes. Are there infinitely many integers $n \not\equiv 0 \pmod 4$ for which the numbers (1) are never squarefree ? In fact is there a single such n ?

I conjectured that if n is such that all the integers (1) are composite and if $p_i^{(n)}$, $1 \leq i \leq \ell$ is the set of all the prime factors of the integers (1) then there are infinitely many integers n_r, $n_1 = n < n_2 < \dots$ for which all the integers $n_r - 2^k$, $k > 1$, $2^k \leq n_r$ have a prime factor among the $p_i^{(n)}$, $1 \leq i \leq \ell$. Perhaps in fact, it is not necessary to consider all the $p_i^{(n)}$, $1 \leq i \leq \ell$ but only a subsequence so that every integer (1) is a multiple of one of the primes of this subsequence. I never got anywhere with these conjectures.

Straus and I considered the following two questions: (A) Is it true that there are infinitely many odd integers n for which all the integers

(2) $$n - k! \;, 2 \leq k, \; k! < n$$

are primes ? On probability grounds, this seemed to us unlikely. Nevertheless it would be nice to find a counter-example to the following conjecture. For every ℓ there is a $p^{(\ell)}$, $\ell! < p^{(\ell)} < (\ell + 1)!$ for which all the integers $p^{(\ell)} - k!$, $2 \leq k \leq \ell$ are primes. Question (B) states: Is it true that there are fnfinitely many odd integers n for which all the integers

$$n - (2k)! \;, 1 \leq k, (2k)! \leq n$$

are primes ? Here on probability grounds we expect the answer to be affirmative and further there probably is for every ℓ, a $p^{(\ell)}$, $(2\ell)! < p^{(\ell)} < (2\ell + 2)!$ for which all the integers $p^{(\ell)} - (2k)!$, $1 \leq k \leq \ell$ are primes. These questions are certainly unattackable by the methods at our disposal.

C. Pomerance, The Prime number Graph, Math. Comp.

C. Pomerance, A Note on the least prime in an arithmetic progression, J. Number Theory (1980).

P. Erdos, In the integers of the form $2^n + p$ and some related problems, Summa Brazil Math. II (1950), 1-11.

R. C. Vaughan, Some applications of Montgomery's sieve, J. Number Theory 5 (1973), -79.

§ III

In this chapter, I discuss miscellaneous problems.

1. One of my oldest problems states: Is it true that almost all integers have two divisors d_1 and d_2 satisfying $d_1 < d_2 < 2 d_1$? In a recent paper Tenenbaum and I obtained significant results on this problem but the final solution still seems to be far away and I offer 500 dollars for a proof or disproof.

Denote by ε_n the density of the integers which have a divisor in $(n, 2n)$. Besicovitch proved $\liminf \varepsilon_n = 0$ and I showed $\varepsilon_n \longrightarrow 0$. Is it true that for every $\varepsilon > 0$, there is an $n_0 = n_0(\varepsilon)$ and an A_ε so that for every $n > n_0$ the number of integers m, $X < m < X + A_\varepsilon \cdot n$ which have a divisor d, $n < d < 2n$ is less than $\varepsilon \cdot A_\varepsilon \cdot n$? This question just occurred to me and I apologise to the reader if it turns out to be trivial or false.

Several related questions can be asked e.g. estimate as well as you can the length of the longest interval $I_{n,\varepsilon}$, which is say in (n^2,n^3) and for which the number of integers m in $I_{n,\varepsilon}$ which have a divisor in $(n,2n)$ is greater than $\varepsilon.I_{n,\varepsilon}$ ((I) is the length of the interval I).

P.Erdós and G.Tenenbaum, Sur la structure de la suite des diviseurs d'un entier, Annales de l'Inst Fourier 31(1981),17-34.

P.Erdős, A.Sarkozy and E.Szemeredi, Individibility properties of sequences of integers, Number Theory, Coll. J.Bolyai Math. Soc., North Holland 1968, 36-49. Both of these papers have many references.

2. Is there an absolute constant $c > 0$ so that for every n there is an interval of length m, $X < m < X + n$ for which every m has a divisor d, $c\,n < d < n$. Ruzsa observed that this holds if $c = O\left(\frac{1}{\log n}\right)$. R.Freud has certain preliminary results on this problem which are not yet in their final form.

3. In p . 51 of I the following problem is stated: Let $A = \{ a_1 < a_2 < \dots \}$ be a basis and put $A_1(x) = \sum_{a_i \leq X} 1$. $A_r(X)$ denotes the number of integers not exceeding X which are the sum of r or fewer A's . Since A is a basis we have for some k , $A_k(X) = X + O(1)$. Assume that $A_1(x) = o(X)$. Is it then true that

$$A_1(X) / A_2(X) \longrightarrow 0? \tag{1}$$

S.Turjanyi pointed out that (1) is incorrect as it stands. Rusza observed that very likely

$$(2) \qquad A_1(X)/A_2(2X) \longrightarrow 0$$

and that (2) probably follows from the results of Freiman.

We all conjectured that if $A_r(X) = o(X)$ then

$$(3) \qquad \lim A_r(X) \ / \ A_{r+1}((r+1)\ X) = 0.$$

G.A.Freiman,

Foundations of a structural theory of set addition, Vol.37, translation of Math. Monographs Amer. Math. Soc. Providence R.I. 1973.

4. In p.29 of I the following problem is stated: Let $n_1 < n_2 < \dots$ be an infinite sequence of integers for which for every choice of the a_i almost all integers satisfy at least one of the congruences $a_i \pmod{n_i}$ (Almost all means all except for a sequence of density 0). Such a sequence $n_1 < n_2 < \dots$ is said to have property P. Is it then true that to every $\varepsilon > 0$ there is a k so th-t for every choice of the a_i the density of integers which do not satisfy any of the congruences $a_i \pmod{n_i}$, $1 \leq i \leq k$ is less than ε .

J.Haight observed that this follows easily from a theorem of C.A.Rogers (H.Halberstam and C.A.Rogers Sequences p.292): For any fixed system $R_1, \dots, R_\ell$ of congruence classes, the density of the union of translates

$$R_1 + t_1, \dots, R_\ell + {=}t_\ell$$

is minimal when these translates have a common element.

This result implies that it suffices to prove that if $n_1 < n_2 < \dots$ is an infinite sequence for which almost all integers are multiples of at least one n_i then for every $\varepsilon > 0$ there is a k for which the density of integers m which are not dividible by any of the n_i, $1 \leq i \leq k$ is less than and the proof of this is not difficult.

Thus Rogers' result gives that the problem really loses interest since property P simply means that almost all integers have a divisor among the n_i.

5. To end this paper I give a random selection of some problems. I ask for the indulgence of the reader if some of them turn out to be trivial or false. First of all here are two questions:R.Freud and I considered very recently: Let $a_1, a_2, \dots$ be a permutation of the integers. Is it true that

$$(1) \qquad \liminf_{n \to \infty} \; (a_n, a_{n+1})/n \leq \frac{1}{2} .$$

It is easy to see that (1) if true is best possible. Freud has a simple proof of (1) with 3/4 instead of 1/2. Is it true that

$$(2) \qquad \limsup_{n \to \infty} \; [a_m , a_{n+1}] / n = \infty.$$

Both (1) and (2) seem extremely obvious and perhaps we overlook a trivial argument. Freud has an example of a permutation of the integers $a_1, a_2, \ldots$ for which

$$[a_n, a_{n+1}] < n \exp((\log n)^{1/2+\varepsilon}).$$

Is it true that for every $T > T_0$ there is a composite n with $n - p(n) < T$ where $p(n)$ is the least prime factor of n? If true determine if possible the largest T for which the result fails? It will surely be easy to find this T but may be difficult to prove this.

Is it true that for every c_1 and c_2 there is a $T_0(c_1, c_2)$ so that for every $T > T_0(c_1, c_2)$ there is a composite n for which

$$n > T + c_1, \quad n - p(n) < T - c_2 ?$$

In fact put

$$\min_{\substack{n > T \\ n \text{ composite}}} (n - p(n)) = T - f(T).$$

Is it true that $f(T) = (1 + o(1))T^{1/2}$?

P.Erdös, On a property of 70, Math. Mag. 51 (1978), 238-290. For many related problems see, P.Erdös, D.E.Penney and C.Pomerance, On a class of relatively prime sequences, J. Number Theory, 9 (1978), 951-974.

Mathematics Institute
The Hungarian Academy of Sciences
Budapest, HUNGARY