ON SOME PROBLEMS IN NUMBER THEORY

P. Erdös

I discuss some problems which have interested me during much of my long life.

1. One of my old conjectures states that almost all integers have two divisors $d_1 < d_2 < 2d_1$. I proved in 1948 that the density of these integers exists but I could never prove that this density is 1. Denote by $\tau(n)$ the number of divisors of n and by $\tau^+(n)$ the number of integers k for which n has a divisor d satisfying $2^k < d < 2^{k+1}$. To prove my conjecture it would suffice to prove that

$$\tau^+(n) < \tau(n) \tag{1}$$

holds for almost all n. In fact I conjectured that $\tau^+(n)/\tau(n) \to 0$ for almost all n. Tenenbaum and I recently disproved this conjecture. In fact, the density of integers n satisfying $\tau^+(n) < \varepsilon\tau(n)$ goes to 0 as $\varepsilon \to 0$. Probably $\tau^+(n)/\tau(n)$ has a continuous distribution function, but so far we were not able to prove this.

The following problem which we could not settle would be of great interest here: Is it true that to every $\varepsilon > 0$ there is a k so that the density of integers n for which n has two divisors $d_1 < d_2 < 2d_1$ so that all prime factors of d_1d_2 are $>k$ is less than ε^2. Probably the conjecture is false.

For the older literature of this question see Halberstam-Roth, "Sequences"; for the more recent papers see our forthcoming paper with Tenenbaum and also the older papers of Tenenbaum.

2. In 1934, Romanoff proved that the lower density of the integers of the form 2^k+p is positive. No doubt the density in question exists but at present this can not be proved. In 1934 Romanoff in a letter asked me if every large odd number is of the form $2^k + p$? Van der Corput and I disproved this and I in fact found an infinite arithmetic progression of odd numbers no term of which is of the form 2^k+p. The question of Romanoff led me to the discovery of

covering congruences, perhaps the most interesting new problem I raised (so far) during my long life: A system of congruences

$$a_i \pmod{n_i} \quad , \quad 1 < n_1 < \ldots < n_k \tag{2}$$

is called covering if every integer satisfies at least one of the congruences (2). The outstanding problem states: Is there a system (2) for which n_1 is as large as we please? k of course would have to tend to infinity probably fairly fast with n_1. Choi found a system (2) with $n_1 = 20$ and this is still our record. I offer a prize of 5000 Francs for a proof or disproof of this conjecture.

I observed already in 1934 that if the conjecture $(n_1 \to \infty)$ is true, then for every r there is an infinite arithmetic progression no terms of which is of the form $2^k+\theta_r$ where θ_r has at most r prime factors.

Is it true that there is an r so that every integer is the sum of a prime and at most r powers of two? This question probably can not be decided by covering congruences. Crocker proved that there are infinitely many odd integers not of the form $2^k + 2^\ell + p$. Linnik and Gallagher proved that to every $\varepsilon > 0$ there is an r so that the lower density of the integers $p + 2^{k_1} + \ldots + 2^{k_r}$ is greater than $1 - \varepsilon$.

For further literature and other related problems, see our forthcoming long paper (book?) with R. L. Graham which will soon appear in Enseignement Math. and which will deal with problems in elementary number theory. To end this chapter I just state one final problem: Is it true that all (or almost all) $n \not\equiv 0 \pmod 4$ are the sum of a power of two and a squarefree number?

3. More than 50 years ago, Van der Waerden proved that if we split the integers into two classes, at least one of the classes contains arbitrarily long arithmetic progressions. He also proved the finite form of this theorem: There is an $f(n)$ so that if we split the integers not exceeding $f(n)$

into two classes, at least one of them will contain an arithmetic progression of n terms. Van der Waerden's upper bound for $f(n)$ seemed very weak: $f(n)$ increased like the function of Ackermann, the nonprimitive recursion function. Berlekamp proved $f(n) > n\,2^n$ and it was always assumed that $f(n)$ increases much slower than Ackermann's function. Solloway was the first to express doubts and I first thought that this is obvious nonsense, but realize now after the surprising results of Paris-Harrington that Solloway's suggestion must be taken seriously. In any case, I offer 500 Francs for the proof or disproof of $\lim_{n\to\infty} f(n)^{1/n} = \infty$. (J. Paris and L. Harrington, A mathematical incompleteness in Peano arithmetic, Handbook of Mathematical Logic, North Holland, Amsterdam, 1977, pp. 113-1142.)

Nearly 50 years ago Turan and I conjectured that if $n > n_0(\varepsilon,k)$ and $1 \le a_1 < \ldots < a_t \le n$, $t > \varepsilon n$, then the a's contain k consecutive terms of an arithmetic progression. This is of course a very significant strengthening of Van der Waerden's theorem. I offered 1000 dollars for a proof or disproof and Szemerédi proved our conjecture in 1972-1973. His proof is a masterpiece of combinatorial reasoning which already had many applications in different branches of combinatorics. A few years ago Furstenberg proved Szemerédi's theorem by methods of ergodic theory and he and Katznelson recently proved the n-dimensional generalization of Szemerédi's theorem. It is not yet possible to say if the importance of ergodic theory in number theory will rival in importance the discovery early last century of analytic number theory.

I conjectured that if $\sum_i \frac{1}{a_i} = \infty$ (a_i integers), then the a's contain, for every k, k consecutive terms of an arithmetic progression. I offer 15000 Francs for a proof or disproof. I often said that I do not expect to have to pay this in my lifetime and that I should leave some money for it when I "leave" (the second "leave" means of course leave on the journey where no visa and passport is required).

Euler proved that $\sum \frac{1}{p} = \infty$, thus my conjecture if true would imply that for every k the primes contain k consecutive terms of an arithmetic progression.

For literature, see our paper with Graham quoted previously.

4. Some Miscellaneous Recent Problems:

Let $1 \le a_1 < \ldots < a_{t_n} \le n$ and assume that $(a_i+a_j) \nmid a_i a_j$. Determine or estimate $\max t_n = f(n)$ as accurately as possible. I conjectured that $\max t_n = (\ + o(1))n$ but Odlyzko proved that $f(1000) \ge 717$ which certainly throws some doubt on my conjecture. Assume now $(a_i+a_j) \nmid 2a_i a_j$ and put $\max t_n = f_1(n)$. Here I thought $f_1(n) = o(n)$, but as far as I know, nothing is known about this.

Silverman and I asked a few years ago. Let $1 \le a_1 < \ldots < a_s \le n$ and assume that a_i+a_j , $1 \le i \le j \le s$ is never a square. Is it true that $\max s = (1 + o(1))\frac{n}{3}$? The integers $\equiv 1 \pmod 3$ show that if true, then this result is best possible. We could get nowhere with this and recently I noticed that the following finite form is also open: Let $a_1, \ldots, a_k$ be residues (mod d) and assume that

$$x^2 \not\equiv a_i + a_j \pmod d \quad , \quad 1 \le i \le j \le k \quad .$$

Is it then true that $k \le \frac{d}{3}$? I could not settle this question, but perhaps I overlook a trivial idea.

Let $f(X,n)$ be the number of integers $X < m \le X+n$ for which there is a p/m , $\frac{n}{3} < p < \frac{n}{2}$. Is it true that $f(X,n) > C\, n/\log n$? It is clear that no such result can hold for $\frac{n}{2} < p \le n$. To see this, put $A = \prod_{\frac{n}{2}<p\le n} p$ and let $X = A - \frac{n}{2}$.

Akademia Matematikai Intezete
Realtanoda u. 13-15
H-1053 Budapest, Hongrie