FAREWELL, PAUL

I was 19 years old, a second year university student, when I received the following letter: "Dear Mr. Sárközy, I have heard about your nice results" so and so "from Paul Turán. Please, come and see me at the Mathematical Institute" (of the Hungarian Academy of Sciences). The letter was signed by Paul Erdős. Probably tens of mathematical careers started with such a letter from him.

I visited him soon at the Mathematical Institute. I told him my results (which were not that exciting but, perhaps, good enough for a beginner) and I sketched the proofs. He made several deep and original comments and at the end he asked a related question. As an answer to this question, I soon published (in the Acta Arithmetica) my first paper based on an Erdős problem.

This first meeting with him was the first "Uncle Paul session" (as his friends and collaborators called them) that I attended, and it was followed by many others. During these sessions, he was usually discussing simultaneously with 2–3 disciples ("epsilons" as he called them) and collaborators working in different fields. Indeed, to match his speed, intensity, ingenuity and knowledge, at least two or three other mathematicians were needed. Even so, when you left after such a session you felt completely squeezed out, unable to ever do mathematics anymore. However, when after a good sleep you awoke next morning your head was full of his problems and ideas, and you were just unable to think about anything else; and in at most two days you were longing again badly for one of those, ever so exhausting, "Uncle Paul sessions".

Three years after our first meeting we wrote our first joint paper which was a triple paper with Endre Szemerédi. This was followed by more than 60 joint papers (nearly half of them were triple or even quadruple papers with E. Szemerédi, V. T. Sós, C. Pomerance, J.-L. Nicolas, C. L. Stewart, C. Mauduit, H. Maier, I. Z. Ruzsa, P. Kiss, J.-M. Deshouillers, M. B. Nathanson and A. M. Odlyzko). During the decades of joint work, our understanding and communication was getting like in a long marriage: one word was enough to tell a long story, exchanging ten sentences was enough to write a joint paper.

Mathematics was his life; he was doing mathematics for 17–18 hours every day. Lately his friends were asking him to slow down a little, to live a less self-consuming life style. His standard answer was: "We can rest enough in the grave." Now he is resting indeed. Farewell, Paul... It is still hard to believe that life will go on, mathematics will survive without you, but it will: mathematics is eternal... Just it will not be the same any more...

András Sárközy

ACTA ARITHMETICA
LXXXI.4 (1997)

Paul Erdős (1913–1996)

by

András Sárközy (Budapest)

BIOGRAPHY OF PAUL ERDŐS

Paul (Pál in Hungarian) Erdős was born in Budapest, Hungary on March 26, 1913. Both his parents were high school mathematics teachers. From 1930 he studied mathematics at the Péter Pázmány (now Eötvös) University in Budapest. At the university his closest friends were Tibor Gallai, Paul (Pál) Turán and George (György) Szekeres. He graduated from the Pázmány University in 1934 (at the age of 21) with a PhD. After graduation the steadily worsening political atmosphere (antisemitism, the approaching fascism) forced him to leave Hungary. Between 1934 and 1938 he lived in Manchester, UK (and in the meantime he visited Hungary three times each year). From 1938 to 1948 he stayed in the US (1938–40: Institute of Advanced Study, 1940–43: University of Pennsylvania, 1943–45: Purdue University, 1945–48: Syracuse University). In 1948 he left for Europe: first he stayed in the Netherlands (for two months), then, after 10 years of absence, he visited Budapest (for two months), finally, he travelled to the UK. After one year (1949–50) in the US, he returned to the UK (1950–51: Aberdeen, 1951–52: London). In 1952–54 he was visiting the Notre Dame University in the US. In 1954, during the McCarthyism, he was interviewed by the Immigration Service. Since he was insisting on his democratic principles and, in particular, on having world wide personal connection with his colleagues, including East European mathematicians, his US reentry permit was denied. Thus after participating in a congress in Amsterdam, he was unable to return to the US, and he lost his "green card" and his Notre Dame job. In the next 9 years he could visit the US just once, participating in a conference with a special short term visa. From 1954 on, he keeps travelling around the Globe, without ever accepting a permanent full time job. In these years he visited Haifa, Israel every year for up to 3 months. Between 1948 and 1955, i.e., during the worst years of Stalinism and post-Stalinism he stayed away from Hungary; in 1955, when a slow improvement started, he visited

Budapest again. Then he made a deal, at that time quite amazing and exceptional, with the Hungarian authorities: from 1955, he was considered a Hungarian citizen and an Israeli resident, and he received a special consular passport which enabled him to cross the Hungarian border at any time in either direction. During his Hungarian visits he stayed at the Mathematical Institute of the Hungarian Academy of Sciences, and at the beginning a special arrangement was made for each of his visits. In 1962, this connection was made more formal: he got a permanent job in the Institute (up to his death). In 1963 the US Immigration reviewed his case and finally he received the American visa (a J-1 visa which he had to renew from time to time). From this point on up to his death, his schedule was nearly the same every year: 4–5 months in Hungary, slightly less in the US, a short trip to Israel, and the rest of the time travelling around the Globe, participating in conferences and giving talks.

He died in Warsaw on September 20, 1996. He died as he lived: travelling and working. He was participating in a combinatorics conference in Poland which ended on Friday, September 20, and he was to leave next day for a number theory conference in Lithuania. However, in the early morning on Friday he got a heart attack and he was taken to a hospital. In the early afternoon he got a second heart attack and this killed him.

Erdős published about 1.500 research papers; it will take years to determine the exact number of his publications and to make a complete list of them. (Euler has been the only more prolific mathematician in the history of mathematics.) As Ernst Straus wrote: "In many ways, Paul Erdős is the Euler of our times. Just as the 'special' problems Euler solved pointed the way to analytic and algebraic number theory, topology, combinatorics, function spaces, etc.; so the methods and results of Erdős's work already let us see the outlines of great new disciplines, such as combinatorial and probabilistic number theory, combinatorial geometry, probabilistic and transfinite combinatorics and graph theory as well as many more yet to arise from his ideas."

He made a contribution of basic importance to modern mathematics not only by proving theorems but also by posing problems, teaching and helping talented young mathematicians and collaborating with hundreds of mathematicians in many different countries and different fields. About 70% of his papers were joint papers; he had nearly 500 coauthors. (No other mathematician has ever had nearly that many coauthors.)

He was the member of 8 scientific academies and received honorary degrees from 15 universities. In 1984 he received the Wolf prize (Israel). Other prizes and awards received by him: Cole Prize (A.M.S.), Kossuth Prize (Hungary), State Prize (Hungary), Gold Medal of the Hungarian Academy of Sciences and Tibor Szele Prize (of the Hungarian Mathematical Society).

THE NUMBERTHEORETIC WORKS OF PAUL ERDŐS

Paul Erdős has published more than 600 papers on number theory. Due to the large number of his results and to his wide interests, it would clearly be a hopeless task to try to give a more or less complete survey of his numbertheoretic works. Thus all one can do is to select and briefly discuss a few of the most important results and problems of his. Even doing so, one needs advice of experts of different fields; in particular, I would like to thank Kálmán Győry, Jean-Louis Nicolas, Attila Pethő, Carl Pomerance, Andrzej Schinzel, Cameron L. Stewart and Vera T. Sós for their valuable comments and suggestions. If, however, any errors are made, important results are overlooked, or certain fields are not represented with the right weight, it is completely the author's fault.

Shortly before his death Erdős wrote two papers [96.03, 97.01] on his favourite problems and results. Since these two papers will often be quoted, reference to them will be distinguished by introducing quotations from them as [FT:] (for the paper [96.03], "On some of my favourite theorems") and [FP:] (for the paper [97.01], "Some of my favorite problems and results"), respectively.

1. Diophantine equations, diophantine approximation. Erdős and Selfridge proved [75.19]:

THEOREM. *The product of* 2 *or more consecutive integers is never a power* (*i.e.*, *never of the form* k^l *where* k, l *are positive integers*, $l \geq 2$).

In 1951 Erdős proved [51.03]:

THEOREM. *If* k, n *are positive integers with* $4 \leq k$, $2k \leq n$, *then* $\binom{n}{k}$ *is not a power.*

He conjectured that the same assertion holds for $k = 2$ and 3 as well. Very recently, this conjecture has been proved for $k = 2$ and $k = 3$ by Darmon and Merel, and Győry, respectively. The following related problem is still open:

[FT:] "Is it true that the product of four or more integers in an arithmetic progression is never a power?

Here Ramachandra, Shorey and Tijdeman have important partial results."

In an early paper Erdős and Turán proved [34.03]:

THEOREM. *There is a positive absolute constant* c *such that if* A *is a finite set of positive integers then*

$$\omega\Big(\prod_{a,a'\in A}(a+a')\Big) > c\log|A| \tag{1}$$

(*where* $\omega(n)$ *denotes the number of distinct prime factors of* n).

They conjectured that the result can be extended to sums $a+b$: if A, B are finite sets of positive integers with

$$|A| = |B| \tag{2}$$

and $|A| \to \infty$, then

$$\omega\Big(\prod_{a\in A}\prod_{b\in B}(a+b)\Big) \to \infty.$$

This conjecture was proved more than 50 years later by Győry, Stewart and Tijdeman who showed that assuming only $|A| \geq |B| \geq 2$ in place of (2), one has

$$\omega\Big(\prod_{a\in A}\prod_{b\in B}(a+b)\Big) > c\log|A|. \tag{3}$$

While the proof of the Erdős–Turán theorem is completely elementary, the crucial tool in the proof of (3) is a deep result of Evertse on an upper bound for the number of solutions of S-unit equations. In [88.09] Erdős, Stewart and Tijdeman gave lower bounds for the number of solutions of S-unit equations. These papers induced further work in this field by Győry, Sárközy, Stewart and Tijdeman.

Erdős and Obláth [37.06] proved that

$$n! = x^k + y^k, \qquad (x,y)=1,\ k>2,$$

has no solutions in positive integers n, k, x, y if $k \neq 4$. (In 1973 Pollack and Shapiro showed that it also has no solutions if $k=4$.)

[FT:] "Turán and I obtained the following result [48.01], important in the theory of uniform distribution:

Theorem. *Let z_ν, $1 \leq \nu < \infty$ be a sequence of numbers in $(0,1)$. Then for every m and $0 \leq \alpha < \beta \leq 1$ we have*

$$\Big|\sum_{\substack{\nu\leq n\\ \alpha<z_\nu\leq\beta}} 1-(\beta-\alpha)n\Big| < c\frac{n}{m+1} + \sum_{j=1}^{m}\frac{1}{j}\Big|\sum_{k=1}^{n} e^{2\pi i j z_k}\Big|."$$

A survey of Erdős's work on irrationality and transcendence is given in the Erdős–Graham book [80.11, Chapter 7]. V. T. Sós is working on a survey of Erdős's work on diophantine approximation.

2. Sums. In this section only sums with two terms are considered.

[FT:] "Now I want to talk about applications of probability methods to additive number theory. More than 60 years ago Sidon posed the following problem:

Let $a_1 < a_2 < \ldots$ be an infinite sequence of integers. Denote by $f(n)$ the number of solutions of $n = a_i + a_j$. Does there exist a sequence $A =$

$\{a_1 < a_2 < \dots\}$ for which $f(n) > 0$ for all $n > n_0$ but $f(n)/n^\varepsilon \to 0$ for every $\varepsilon > 0$?

At first I thought that this problem is easy but it took me 20 years to prove by probabilistic methods that

THEOREM. *There is a sequence A for which*

$$c_1 \log n < f(n) < c_2 \log n.\text{''} \tag{4}$$

This is proved in [56.10]. Erdős and Rényi [60.01] gave further applications of this probabilistic method.

[FT:] "Nathanson, Tetali and I have several further related results all of which will soon be published.

To illustrate some limitations of the probability method let me just state two plausible conjectures which have resisted so far all attacks:

1. Turán and I conjectured that if $f(n) > 0$ for all $n > n_0$, then $\limsup f(n) = \infty$. Perhaps even the following stronger result holds:

$$\limsup \frac{f(n)}{\log n} > 0.$$

In other words, (4) is best possible in a very strong form. For the details of the proof of (4) I refer to the excellent book of Halberstam and Roth: *Sequences*.

2. Sárközy and I conjectured that there is no function f for which

$$\frac{f(n)}{\log n} \to c \qquad (0 < c < \infty). \tag{5}$$

These conjectures indicate that (4) is best possible. (...) We proved [85.09] that

THEOREM. *There is no f for which*

$$\frac{|f(n) - \log n|}{\sqrt{\log n}} \to 0$$

which is of course much weaker than (5)."

Erdős and Sárközy also proved [86.05] that if the function $F(n)$ is "smooth" in a well-defined sense (the details are too complicated to present them here), then there is a sequence A for which

$$f(n) - F(n) = O(\sqrt{F(n)\log n}).$$

(This generalizes (4).)

Erdős continues: "Turán and I investigated the following problem: Denote by $f(n) = \max \sum_{a_i < n} 1$, if $a_i + a_j$ are all distinct." (In this case $\{a_1, a_2, \dots\}$ is said to be a *Sidon set*.) Then

Theorem.

$$f(n) = (1 + o(1))n^{1/2}.$$

Here perhaps $f(n) = n^{1/2} + O(1)$ is too optimistic, $f(n) = n^{1/2} + O(n^{\varepsilon})$ should be true but will be difficult.

For many further results and problems on this topics see Halberstam–Roth: *Sequences*, and many of my papers. See also our papers with Sárközy and V. T. Sós [85.08, 86.06, 87.10, 94.01] and Nathanson and Tetali [95.02]."

Erdős and Freud [91.05], resp. Erdős, Sárközy and V. T. Sós [94.04, 95.05] studied sum sets of Sidon sets (very recently some of the results in the last two papers have been sharpened by Ruzsa, and Spencer and Tetali).

[FT:] "I should not forget our result with W. Fuchs [56.04] which certainly will survive the authors by centuries:

Theorem. *Let* $a_1 < a_2 < \ldots$ *be an infinite sequence of integers. If* $F(x)$ *denotes the number of solutions of* $a_i + a_j < x$, *then*

$$F(x) = cx + o\left(\frac{x^{1/4}}{(\log x)^{1/2}}\right) \tag{6}$$

is impossible.

Jurkat and later Montgomery and Vaughan proved that $o(x^{1/4})$ is also impossible in (6)."

[FT:] "I proved [36.06, 54.02] that

Theorem. *Every basis is an essential component.*

Linnik was the first to give an essential component which is not a basis. Plünnecke and in particular Ruzsa have the best results in this subject at the moment."

Erdős had numerous other papers on (additive) bases, written partly jointly with Deshouillers, Graham, Nathanson, Newman and Sárközy.

We mentioned the classical Erdős–Turán result (1) on prime factors of sums. Erdős studied the distribution of prime factors and other arithmetic properties of sums $a+b$ jointly with Maier, Pomerance, Sárközy and Stewart [77.07, 78.06, 87.04, 87.07, 93.03].

3. Partitions. If $A = \{a_1 < a_2 < \ldots\}$ is a finite or infinite sequence of positive integers then let $p(A, n)$ denote the number of solutions of

$$x_1 a_1 + x_2 a_2 + \ldots = n$$

in non-negative integers x_i, and write $p(\mathbb{N}, n) = p(n)$.

[FT:] "I would like to mention my result with Lehner. We prove [41.03] that

Theorem. *If $p_k(n)$ denotes the number of partitions of n which have fewer than k summands, then if*

$$k = \frac{1}{C}\sqrt{n}\log n + x\sqrt{n},$$

then

$$\lim \frac{p_k(n)}{p(n)} = \exp\left(-\frac{2}{C}e^{-\frac{1}{2}Cx}\right)."$$

(So that almost all partitions have $c\sqrt{n}\log n$ summands.)

Erdős and Bateman [56.02] proved:

Theorem. *$p(A,n)$ is strictly increasing for all large n if and only if the following condition is satisfied*: $|A| > 1$ *and if any element is removed from A, then the remaining elements have greatest common divisor* 1.

Consider a partition π of n into a's:

$$a_{i_1} + a_{i_2} + \ldots + a_{i_k} = n, \qquad i_1 \le i_2 \le \ldots \le i_k.$$

If the positive integer b can be written in the form

$$\varepsilon_1 a_{i_1} + \varepsilon_2 a_{i_2} + \ldots + \varepsilon_k a_{i_k} = b \quad \text{with } \varepsilon_j \in \{0,1\} \quad \text{for } j = 1,2,\ldots,k,$$

then we say that the *partition π represents b*.

In the case $A = \mathbb{N}$ Erdős and Szalay [83.06] proved:

Theorem. *Almost all partitions of n represent all the integers* $1,\ldots,n$. *Moreover, almost all the partitions π of n that fail to represent at least one $1 \le b \le n$ are the partitions without any* 1 *in π.*

Erdős and Nicolas [95.04] extended this theorem to sets $A \ne \mathbb{N}$.

For $A = \mathbb{N}$ let $R(n,b)$ denote the number of partitions of n which do not represent b. This function $R(n,b)$ has been studied by Erdős, Dixmier, Nicolas and Sárközy [89.10, 90.10, 91.09, 92.07].

Erdős, Nicolas and Szalay [89.11] studied partitions into parts which are unequal and large.

Other partition problems were studied by Erdős and Richmond [76.03, 78.08, 78.15], Alladi, Erdős and Hoggatt [78.05], and Erdős and Loxton [79.11]. Erdős and Graham [72.03] studied a problem of Frobenius.

4. Subset sums. If $A = \{a_1, a_2, \ldots\}$ is a finite or infinite set of integers (or more generally, of elements of a semigroup) and $B \subset A$, then the sum

$$\sum_{b\in B} b = \sum_i \varepsilon_i a_i \quad (\text{where } \varepsilon_i = 0 \text{ for } a_i \notin B \text{ and } \varepsilon_i = 1 \text{ for } a_i \in B)$$

is called a *subset sum* of A. Denote the counting function of A by $A(x)$:

$$A(x) = \sum_{\substack{a \le x \\ a \in A}} 1.$$

Erdős [62.03] proved that

Theorem. *If A is an infinite sequence of positive integers such that*

$$A(x) > x^{(\sqrt{5}-1)/2} \qquad \textit{for } x > x_0,$$

then the set of the subset sums of A contains an infinite arithmetic progression.

(In other words, there is an infinite arithmetic progression all of whose terms can be represented in the form $\sum_{a \in A} \varepsilon_a a$ with $\varepsilon_a = 0$ or 1, $\sum_{a \in A} \varepsilon_a < \infty$.) Later this result was sharpened by Folkman and now Hegyvári has the best estimate.

Erdős and coauthors proposed the study of representations of

(i) squares (Erdős),
(ii) integers taken from a certain interval (Erdős and Graham),
(iii) powers of 2 (Erdős and Freud),
(iv) squarefree integers (Erdős and Freud)

by subset sums of "dense" sets of integers. In particular, problems (iii) and (iv) were studied first by Erdős and Freiman [90.12]. These questions are closely connected with the study of long arithmetic progressions, resp. long blocks of consecutive integers in subset sums of "dense" (finite) sets. Partly the four problems above, partly arithmetic progressions in subset sums have been studied by Erdős, Nathanson and Sárközy [88.10], Alon, Freiman, Károlyi, Lev and Lipkin. Arithmetic progressions in subset sums of "thin" (finite) sets have been studied by Erdős and Sárközy [92.01]. Alon and Erdős [96.02] studied the Ramsey type version of problem (ii) above. Erdős, Sárközy and Stewart [94.03] estimated large prime factors of subset sums.

Erdős and Heilbronn [64.05] proved the following

Theorem. *If p is a prime and $a_1, a_2, \dots, a_k$ are distinct residues modulo p with $k \ge 3(6p)^{1/2}$, then every residue class can be represented in the form $\sum_{i=1}^{k} \varepsilon_i a_i$, $\varepsilon_i = 0$ or 1.*

This result has been sharpened and extended by Hamidoune, Olsen, Ryavec, Sárközy and Szemerédi.

Erdős and Straus [70.03] and Erdős and Sárközy [90.03] studied *non-averaging sets*, i.e., sets such that no element is the arithmetic mean of any subset with more than one element.

Erdős [62.07] and Straus called a set *admissible* if subset sums of subsets of different cardinality are distinct, and they estimated the maximal size of an admissible set selected from $\{1, 2, \ldots, n\}$. Their estimates were improved by Erdős, Nicolas and Sárközy [91.09], and recently Deshouillers and Freiman have settled the problem nearly completely.

5. Products. A set $A = \{a_1, a_2, \ldots\}$ of positive integers is said to be a *multiplicative Sidon set* if the products $a_i a_j$ with $i \le j$ are all distinct. Let $F(n)$ denote the maximal cardinality of a multiplicative Sidon set selected from $\{1, 2, \ldots, n\}$. Erdős proved [38.03, 69.08]

THEOREM. *There exist positive absolute constants c_1, c_2 such that for $n > n_0$ we have*

$$c_1 n^{3/4} (\log n)^{-3/2} < F(n) - \pi(n) < c_2 n^{3/4} (\log n)^{-3/2}.$$

This is a beautiful application of combinatorics: the upper estimate is based on a lemma on cycles of length 4 in bipartite graphs.

Erdős, Sárközy and V. T. Sós [95.03] studied the solvability of the equation

$$a_1 a_2 \ldots a_k = x^2, \qquad a_1, a_2, \ldots, a_k \in A$$

in "dense" sets A (for k fixed); this problem is closely related to the theorem above.

In 1960 Erdős [60.03] proved the following

THEOREM. *The number of distinct integers of the form a, b where $a, b \in \mathbb{N}$, $a, b \le x$ is $x^2 (\log x)^{-\alpha + o(1)}$, where $\alpha = 1 - \log(e \log 2)/\log 2$ $(= 0.0860\ldots)$.*

He proved [65.06] the multiplicative analog of the Erdős–Turán conjecture mentioned in Section 2: Let $A\{a_1, a_2, \ldots\}$ be an infinite set of positive integers, and denote the number of solutions of $a_i a_j = n$ by $g(n)$.

THEOREM. *If $g(n) > 0$ for all $n > n_0$ then*

$$\lim_{n \to \infty} \sup g(n) = \infty.$$

Nešetřil and Rödl, and Nathanson, have extended this result in various directions.

A result involving both sums and products: [FT:] "Szemerédi and I investigated the following surprising phenomenon [83.07]. Let $a_1, a_2, \ldots, a_n$ be a sequence of integers. Consider the products and sums, i.e., all the integers of the form

$$a_i + a_j, \quad \text{or} \quad a_i a_j, \qquad 1 \le i \le j \le n. \tag{7}$$

Denote by $f(n)$ the largest integer so that for every $\{a_1, a_2, \ldots, a_n\}$ there are at least $f(n)$ distinct integers of form (7). We have proved that

Theorem.
$$n^{1+c_1} < f(n) < n^2 e^{-c_2 \log n / \log\log n}.$$

We think that the upper bound is nearer to the truth." Recently this result has been sharpened and extended in various directions by Nathanson, Nathanson and Tenenbaum, Erdős and Szemerédi, and Elekes.

Erdős, Sárközy and V. T. Sós [89.07], and Erdős and Sárközy [90.02] studied the representations of integers by monochromatic sums and products, respectively.

6. Divisors, multiples, coprimality. [FT:] "On divisibility of sequences of integers one of my first result states:

Theorem. *Let $a_1 < a_2 < \ldots$ be a primitive sequence* (*i.e.*, *no a_i divides any other*). *Then*

$$\sum_k \frac{1}{a_k \log a_k} < c \tag{8}$$

with an absolute constant c,

and I conjectured that the left hand side of (8) is the maximum if the a's are the primes. (Zhang and I have some partial results [93.09].) Sárközy, Szemerédi and I [69.10, 70.04] proved that if $a_1 < a_2 < \ldots$ is such that $(a_i, a_j) \neq a_k$, then (8) also holds. Zhang and I conjectured that the maximum is assumed if the a's are the primes and their powers [93.09, 93.10]." Erdős, Sárközy and Szemerédi [67.04, 67.05] also sharpened Behrend's theorem on the estimate of $\sum_{a_i \le x} 1/a_i$ for primitive sequences $a_1 < a_2 < \ldots$

[FT:] "H. Davenport and I proved in 1935 [36.04, 51.04] that

Theorem. *For any sequence $a_1 < a_2 < \ldots$ the set of multiples always has a logarithmic density which equals the lower density.*

Sárközy, Szemerédi and I obtained 30 years later many stronger results [70.04, 70.07]."

[FT:] "On divisibility I proved [36.01] that

Theorem. *If $\varepsilon_n \to 0$ arbitrarily slowly and $n \to \infty$, then the density of integers which have a divisor in $(n, n^{1+\varepsilon_n})$ tends to 0.*

This is a best possible strengthening of a result of Besicovitch." Tenenbaum gave sharp bounds for the density in terms of ε_n.

[FT:] "I proved [48.04] that for the set of integers which have two divisors d_1 and d_2 with $d_1 < d_2 < 2d_1$ the density exists. I conjectured 60 years ago that this density is 1. This and much more was proved about 10 years ago by Maier and Tenenbaum. For more results in this subject see Halberstam–Roth: *Sequences* and Hall–Tenenbaum: *Divisors*."

Erdős, partly jointly with Hall, Herzog, Nicolas, Schönheim and Tenenbaum, studied the distribution of divisors in [65.04, 70.01, 70.08, 75.17, 76.25, 77.13, 78.10, 79.16, 81.15, 83.11, 89.18, 96.04].

He conjectured [62.08] that for $n, k \in \mathbb{N}$, the largest subset of $\{1, 2, \ldots, n\}$ not containing $k+1$ pairwise coprime integers is the set consisting of the multiples of the first k primes. Erdős, Sárközy and Szemerédi [69.02, 80.14, 93.05] and Szabó and Tóth proved partial results and other related theorems. Recently Ahlswede and Khachatrian have settled the problem by disproving the conjecture in its original form and showing that it is true in a slightly weaker form.

Other coprimality related problems are studied in [62.02, 65.09, 70.08, 77.03, 78.04].

7. Primes. [FT:] "Selberg and I [49.01] gave an elementary proof of the prime number theorem in 1948. (...) The starting point of the whole work was the fundamental inequality of Selberg

$$\sum_{p<x} (\log p)^2 + \sum_{pq<x} \log p \log q = x \log x + O(x) \tag{9}$$

for which Selberg found an ingenious elementary proof. Here I just want to state my new type Tauberian theorem which is related to (9).

THEOREM. *Let* $a_k > 0$, $s_m = \sum_{k=1}^{m} a_k$. *Assume*

$$\sum_{k=1}^{n} a_k (s_{n-k} + k) = n^2 + O(n). \tag{10}$$

Then

$$s_n = n + O(1). \tag{11}$$

My proof of (11) was very complicated [49.02]. It was simplified by Siegel and later generalized and simplified by H. Shapiro. I have many more papers on Tauberian theorems, one with Karamata [56.08].

I gave a lecture on this topic in Urbana, Illinois and Hua (who had attended my lecture) asked what happens if we assume $\sum_{k=1}^{n} k a_k = \frac{1}{2} n^2 + O(n)$ instead of (10). I proved [49.10] that $s_n = n + O(\log n)$. The other question is when we replace (10) by $\sum k s_{n-k} = \frac{1}{2} n^2 + O(n)$. Then $s_n = n + o(n)$. I also proved that $s_n = n + o(\sqrt{n})$ is not true. Korevaar conjectured that the right order of magnitude in this second case is $s_n = n + O(\sqrt{n})$ and he proved $s_n = n + O(n^{1/2+c})$ for any $c > 0$." Hildebrand and Tenenbaum have recently proved another related Tauberian theorem.

Let p_n denote the nth prime. [FT:] "Put $d_n = p_{n+1} - p_n$. I proved in 1934 [35.07] that

Theorem. *For infinitely many* n

$$d_n > \frac{c \log n \log\log n}{(\log\log\log n)^2}, \tag{12}$$

and in 1938 Rankin added a factor $\log\log\log\log n$ to the numerator":

$$d_n > \frac{c \log n \ \log\log n \ \log\log\log\log n}{(\log\log\log n)^2}. \tag{13}$$

Later Maier and Pomerance, and recently Pintz improved on the value of the constant c in this inequality.

[FT:] "Turán and I proved in 1948 [48.03] that

Theorem. *The density of integers for which* $d_{n+1} > (1+\varepsilon)d_n$ *is positive. The same holds if we assume* $d_n > (1+\varepsilon)d_{n+1}$.

Ricci and I proved that the set of limit points of $d_n/\log n$ has positive measure. (I am convinced that it is everywhere dense in $(0,\infty)$.) I can also prove that the set of limit points of d_n/d_{n+1} has positive measure and I am convinced that it is also everywhere dense in $(0,\infty)$. Maier has the sharpest partial results."

Erdős and Pomerance [86.04] studied problems of statistical nature related to primality testing.

Additive problems involving primes are studied in [35.08, 37.04, 37.05, 38.02, 39.08, 50.04].

[FT:] "... denote by $P(n)$ the greatest prime factor of n. Is it true that the density of the integers for which $P(n+1) > P(n)$ is $1/2$? This problem seems unattackable. Pomerance and I have some much weaker results [78.12]."

[FT:] "Consider the greatest prime factor of $\prod_{k=1}^{x} f(k)$. Chebyshev proved that for the greatest prime factor p of $\prod_{k=1}^{x}(1+k^2)$, $p/x \to \infty$. Nagell proved that for every irreducible polynomial f the largest prime factor of $f(1)f(2)\ldots f(x)$ is greater than..." $x(\log x)^{1-\varepsilon}$, and by using his method, $> cx \log x$ can also be proved. "$(\ldots)$ I improved this to $x(\log x)^{c \log\log\log x}$ [52.03]. Schinzel and I [90.08] improved this result and Tenenbaum has the currently sharpest estimate. Very likely the greatest prime factor is $> x^{1+c}$." Recently, Schinzel has given a survey of Erdős's work on arithmetical properties of polynomials (in the same volume where Erdős's paper [FP] appeared); this survey also covers Erdős's work on cyclotomic polynomials.

Erdős, partly jointly with Ecklund, Eggleton, R. Graham, H. Gupta, Khare, Lacampagne, Pomerance, Ruzsa, Sárközy, Selfridge, Straus and Turk [34.01, 55.02, 67.10, 71.02, 73.07, 74.01, 75.10, 76.18, 76.19, 76.23, 76.24, 78.13, 79.09, 80.04, 82.06, 83.01, 84.06, 85.10, 93.01], studied the prime factor structure of consecutive integers and binomial coefficients.

Prime factors of Mersenne numbers and the numbers $n! + 1$ were estimated by Erdős and Shorey [76.17], Erdős, Kiss and Pomerance [91.03], and Erdős and Stewart [76.16].

He studied sieve methods, partly jointly with Jabotinsky, Rényi and Ruzsa, in [49.03, 58.05, 58.06, 68.06, 80.18]. It should be noted here that one of his favourite tools was Brun's sieve; he used it with great ingenuity and effectiveness.

Finally, Canfield, Erdős and Pomerance [83.04] studied the distribution of "smooth" numbers (numbers all of whose prime factors are small). Their results have been superseded by Maier, Hildebrand and Tenenbaum; however, the method worked out by them still has many applications due to its flexibility.

8. Arithmetic functions. Let $\omega(n)$, $\Omega(n)$, $\sigma(n)$, $\varphi(n)$ and $d(n)$ denote the number of distinct prime factors of n, the number of prime factors of n counted with multiplicity, the sum of divisors of n, Euler's function, and the divisor function, respectively. If $\sigma(n) = 2n$, then n is said to be *perfect*, n is *abundant* if $\sigma(n) > 2n$ and is *deficient* otherwise.

[FT:] "Behrend, Chowla and Davenport—using Fourier analysis—proved that the density of abundant numbers exists. I independently gave a different proof, using elementary methods [34.04]. A number n is called *primitive abundant* if n is abundant but no divisor of n is abundant. Denote by $A(x)$ the number of primitive abundant numbers not exceeding x. I proved that

$$\frac{x}{\exp(c_1(\log x \, \log\log x)^{1/2})} < A(x) < \frac{x}{\exp(c_2(\log x \, \log\log x)^{1/2})}.$$

Ivić simplified the proof and obtained better constants. Very recently Avidon improved this (...) The problem if there is an asymptotic formula

$$A(x) = \frac{x}{\exp((1+o(1))c(\log x \, \log\log x)^{1/2})}$$

is still open. Perhaps one could prove that $A(2x)/A(x)$ tends to 2. The sum of the reciprocals of primitive abundant numbers is thus convergent and therefore the density exists. Later I proved that the distribution function of $\sigma(n)$ and $\nu(n)$ are purely singular."

[FT:] "(...) in 1935 I proved that the density of integers n for which $\omega(n) > \log\log n$ is $1/2$ [37.02]. Also I proved that

THEOREM. *The density of integers for which $\varphi(n) > \varphi(n+1)$, $\sigma(n) > \sigma(n+1)$ or $d(n) > d(n+1)$ is $1/2$.*

I used Brun's method and the central limit theorem (which I did not know at that time) for the binomial case. This was easy without using probability theory. (...)

In March of 1939 Kac gave a talk at the Institute of Advanced Study. He stated the following conjecture:

Let $f(n)$ be an additive function for which $|f(p)| < 1$, $f(p^\alpha) = f(p)$ (this is only assumed for the sake of simplicity),

$$\sum_{p<x} \frac{f(n)}{p} = A(x), \qquad \sum_{p<x} \frac{f^2(p)}{p} = B(x), \qquad B(x) \to \infty.$$

The density of integers n for which

$$f(n) < A(n) + c\sqrt{B(n)}$$

is

$$\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{c} e^{-x^2/2}\, dx.$$

He further stated that he can prove it if $f(n) = \sum_{p|n} f(p)$ is replaced by $f_k(n) = \sum_{p|n,\, p<p_k} f(p)$.

I realized that if Kac can prove this, then I can prove his conjecture by using Brun's method. After the lecture we got together and saw that if we combine our knowledge, i.e., the central limit theorem and Brun's method then we can prove the conjecture, and thus with a little impudence we would say that probabilistic number theory was born [39.09, 40.06].

Using our theorem with Kac, Wintner and I proved [39.01] that

Theorem. *The convergence of the three series*

$$\sum_{|f(p)|\ge 1} \frac{1}{p}, \qquad \sum_{|f(p)|\le 1} \frac{f(p)}{p}, \qquad \sum_{|f(p)|\le 1} \frac{(f(p))^2}{p}$$

is both necessary and sufficient for the existence of the distribution function. (...)

I never succeeded to find a necessary and sufficient condition for the absolute continuity of the distribution function and perhaps there is no reasonable condition. I also never could decide if the (purely singular) distribution function of $\varphi(n)$ can have anywhere a (finite) positive derivative (or even a one sided derivative). Diamond and I have a long paper on these questions [78.01]."

[FT:] "I proved in 1944 that if $f(n)$ is additive and $f(n+1) \ge f(n)$ for all large n, then $f(n) = c\log n$. Similarly, if $f(n+1) - f(n) \to 0$, then $f(n) = c\log n$." This result was extended in various directions by Kátai, K. Kovács, Wirsing and others.

Erdős and Nicolas [81.14], Erdős, Pomerance and Sárközy [85.04, 87.05, 87.06], Erdős and Sárközy [94.02] studied the local behaviour of the arithmetic functions $\omega(n)$, $\Omega(n)$, $d(n)$, $\varphi(n)$, $\sigma(n)$.

In [48.06] Erdős estimated the number of integers n with $\omega(n) = k$, $n \le x$, and $\Omega(n) = k$, $n \le x$ respectively. These results were sharpened and extended later by Sathe, Selberg, Erdős and Sárközy [80.17], Balazard, Delange, Halász, Hildebrand, Nicolas, Pomerance and Tenenbaum.

He wrote nearly hundred further papers on arithmetic functions (partly jointly with Alaoglu, Alladi, Babu, Diamond, Elliott, Galambos, Hall, Indlekofer, Ivić, Kátai, Mirsky, Nicolas, Pomerance, Rényi, Ruzsa, Ryavec, Sárközy, Schinzel, Vaaler and others). Some of his work on this subject is discussed in the books of Elliott, *Probabilistic Number Theory* and Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory.*

9. On Erdős's problems. Erdős contributed to the advance of modern number theory at least as much by posing good problems as by proving good theorems. Numerous (probably several thousand) papers have been inspired by his questions, and some of these questions opened up new directions in number theory. A survey of his work would not be complete without presenting at least a few selected Erdős problems.

Problem 1. (His very first problem.) [FP:] "My first serious problem was formulated in 1931 and it is still wide open. Denote by $f(n)$ the largest number of integers $1 \le a_1 < \ldots < a_k \le n$ all of whose subset sums $\sum_{i=1}^{k} \varepsilon_i a_i$ are distinct, where $\varepsilon_i = 0$ or 1. The powers of 2 have this property and I conjectured that

$$f(n) < \frac{\log n}{\log 2} + c$$

for some absolute constant c. I offer \$500 for a proof or disproof. The inequality

$$f(n) < \frac{\log n}{\log 2} + \frac{\log\log n}{\log 2} + c_1$$

is almost immediate, since there are 2^k sums of the form $\sum_i \varepsilon_i a_i$ and they must be all distinct and all are less than kn. In 1954, Leo Moser and I [56.10] proved by using the second moment method that

$$f(n) < \frac{\log n}{\log 2} + \frac{\log\log n}{2\log 2} + c_2$$

which is the current best upper bound.

Conway and Guy found 24 integers all $\le 2^{22}$ for which all subset sums are distinct, which implies $f(2^n) \ge n+2$ for $n \ge 22$. Perhaps

$$f(2^n) \le n+2 \quad \text{for all } n?"$$

Problem 2. (His most "valuable" problem.) Erdős often offered awards for solutions of his problems; in number theory, these awards ranged between 10 and 10.000 dollars. There is just one numbertheoretic problem for whose solution he offered \$10.000, and this is related to the Erdős–Rankin result (13). [FT:] "I offered 10.000 dollars for a proof that (13) holds for every c.

(...) I would like to reduce the offer of 10.000 dollars to 5.000 and offer 10.000 for the proof of $d_n > (\log n)^{1+c}$."

Problem 3. (His most "costly" problem.) In 1936, Erdős and Turán conjectured that van der Waerden's well-known theorem (on the existence of long monochromatic arithmetic progressions in any k-colouring of the integers) can be sharpened in the following way: if for $k \in \mathbb{N}$, $n \in \mathbb{N}$, $r_k(n)$ denotes the maximal number of integers that can be selected from $\{1, 2, \dots, n\}$ so that they do not contain an arithmetic progression of length k, then for every fixed k we have $r_k(n) = o(n)$. Erdős offered an award of 1.000 dollars for proving this conjecture. First Roth in 1953 and Szemerédi in 1969 settled the $k = 3$ and $k = 4$ special cases, respectively, and finally, in 1975 Szemerédi proved the conjecture in its most general form, earning 1.000 dollars in this way; this is the largest award ever paid by Erdős for the solution of a numbertheoretic problem. In 1977, Fürstenberg gave another proof for Szemerédi's theorem.

This conjecture of Erdős and Turán inspired numerous papers, and still there are several related unsolved problems. In particular, Erdős writes: [FP:] "Many years ago I made the following conjecture which, if true, would settle the problem: Let $a_1 < a_2 < \dots$ be a sequence of integers satisfying

$$\sum_{k=1}^{\infty} \frac{1}{a_k} = \infty.$$

Then the a_k's contain arbitrarily long arithmetic progressions. I offer \$5.000 for a proof (or disproof) of this. Neither Szemerédi nor Fürstenberg's methods are able to settle this but perhaps the next century will see its resolution."

Problem 4. (His favourite problem.) [FP:] "Perhaps my favourite problem of all concerns covering congruences. It was really surprising that it had not been asked before. A system of congruences

$$a_i \pmod{n_i}, \quad n_1 < n_2 < \dots < n_k \tag{14}$$

is called a *covering system* if every integer satisfies at least one of the congruences in (14). The simplest covering system is $0 \pmod 2$, $0 \pmod 3$, $1 \pmod 4$, $5 \pmod 6$ and $7 \pmod{12}$. The main problem is: Is it true that for every c one can find a covering system all of whose moduli are larger than c? I offer \$1.000 for a proof or disproof.

Choi found a covering system with $n_1 = 20$, and a Japanese mathematician" (R. Morikawa) "found such a system with $n_1 = 24$."

There are many further partial results and other related results proved by Erdős, Fraenkel, Mirsky, Newman, Schinzel, Selfridge, Znam and others (a survey of this field is given in Chapter 3 of [80.11]).

Problem 5. (The author's favourite Erdős problem.) [FP:] "Now the following problem is annoying: Let $1 < \alpha_1 < \alpha_2 < \dots$ be a sequence of real numbers and assume that for all $i \neq j$, k we have

$$|k\alpha_i - \alpha_j| \geq 1. \tag{15}$$

Note that if the α_i's are integers then (15) implies that no α_i divides any α_j, $i \neq j$." (See Section 6.) "Does (15) imply

$$\sum_i \frac{1}{\alpha_i \log \alpha_i} < \infty \quad \text{or} \quad \frac{1}{\log x} \sum_{\alpha_i < x} \frac{1}{\alpha_i} \to 0 \quad \text{as } x \to \infty?\text{"} \tag{16}$$

(In [FP] the corresponding formulas appear with two misprints, the correct form is (16) above.) Haight has a partial result. However, a construction of Alexander warns that some caution is needed in extending a problem of this type from integers to real numbers. (See [80.11, pp. 84 and 99].)

Problem 6. (A diophantine problem.) Erdős studied unit fractions in numerous papers; a survey of this field is given in Chapter 4 of [80.11]. In particular, Erdős and Straus conjectured that for all $n > 1$, the equation $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = \frac{4}{n}$ has positive integer solutions. It is known that this equation is solvable for $n \leq 10^8$, and Vaughan and Webb have each given estimates for the number of integers n for which $n \leq N$ and this equation is not solvable. Schinzel and Sierpiński extended the problem by conjecturing that the equation $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = \frac{a}{n}$ is always solvable for $n > n_0(a)$. Schinzel also conjectured that for every $a > 1$ there is an $n(a)$ such that all fractions $\frac{a}{n}$ with $n > n(a)$ can be written in the form

$$\frac{1}{x} \pm \frac{1}{y} \pm \frac{1}{z} = \frac{a}{n}$$

with x, y and z positive integers; this is known to be true for all $a < 40$. (See [80.11, p. 44].)

*

Erdős wrote more than 30 problem papers on number theory. The unsolved problems presented in the Erdős–Graham book [80.11] played a role of basic importance in the advance of combinatorial number theory. The majority of the problems discussed in these papers and book are still open.

Eötvös Loránd University
Department of Algebra and Number Theory
Múzeum krt. 6–8
H-1088 Budapest, Hungary
E-mail: sarkozy@cs.elte.hu

Received on 15.4.1997
and in revised form on 9.5.1997 (3183)