

Paul Erdős — Life and Work

Béla Bollobás

Department of Pure Mathematics and Mathematical Statistics, 16 Mill Lane,
Cambridge, CB2 1SB, England

Dipping into the mathematical papers of Paul Erdős is like wandering into *Aladdin's Cave*. The beauty, the variety and the sheer wealth of all that one finds is quite overwhelming. There are fundamental papers on number theory, probability theory, real analysis, approximation theory, geometry, set theory and, especially, combinatorics. These great contributions to mathematics span over six decades; Erdős and his collaborators have left an indelible mark on the mathematics of the 20th century. The areas of probabilistic number theory, partition calculus for infinite cardinals, extremal combinatorics, and the theory of random graphs have all practically been created by Erdős, and no-one has done more to develop and promote the use of probabilistic methods throughout mathematics.

Erdős is the mathematician *par excellence*: he thrives on mathematics, living in a state of continuous excitement; he raises, answers and communicates questions, picking up the problems of others and making incisive contributions to them with lightning speed.

Considering what a mild-mannered man he is, it is surprising that everything about Erdős and his mathematics is extreme. He has written over 1400 papers, more than any mathematician since Euler, and has more than 400 coauthors. If the *Guinness Book of Records* had categories related to mathematical activities, Paul Erdős would hold many of the records by a margin one could not even attempt to estimate, like the thousands of problems posed, the millions of miles travelled, the tens of thousands of mathematical discussions held, the thousands of different beds slept in, the thousands of lectures delivered at different universities, the hundreds of mathematicians helped, and so on.

Today we live in the age of big mathematical theories, bringing together many sophisticated branches of mathematics. These powerful theories can be very successful in solving down-to-earth problems, as in the case of Andrew Wiles's wonderful proof of *Fermat's Last Theorem*. But no matter how important and valuable these big theories are, they cannot constitute all of mathematics. There are a remarkable number of basic mathematical questions that we would love to answer (nay, we *should* answer!) which seem to withstand all our assaults. There is a danger that we turn our backs on such questions, persuading ourselves that they are not interesting when in fact we mean only that we cannot tackle them with our favourite theories. Of course, such an attitude would not be in the proper spirit of science; surely, we should say that we do want to answer these questions, by *whatever means*. And if

there are no theories to help us, no bulldozers to move the earth, then we must rely on our bare hands and ingenuity. It is not that we do not want to use big theories to crack our problems, but that the big theories around are unable to say anything deep about our questions. And, with luck, our hands-on approach will tie up with available theories or, better still, will lead to new, more sensitive theories.

Ernst Straus, who as a young man was Einstein's assistant, reported that the reason why Einstein had chosen physics over mathematics was that mathematics was so full of beautiful and attractive questions that one might easily waste one's life working on the "wrong" questions. Einstein was confident that in physics he could identify the "central" questions, and he felt that it was the duty of a scientist to pursue these questions and not let himself be seduced by any problem – no matter how difficult or attractive it might be.

The philosophy of Erdős has been completely different. Throughout his long career, he has been happy to pursue the beautiful problems he encountered, and has raised many others. But this is not an *ad hoc* process: Erdős has an amazing instinct for discerning beautiful problems that, while appearing innocuous, in fact go right to the heart of the matter. These problems are not chosen indiscriminately; they frequently lead to the discovery of unexpected and exciting phenomena. Like Ramanujan, Erdős uses particular instances of problems to explore an area. Rather than taking whole countries in one sweeping move, he prefers first to occupy some nearby castles, from which he can weigh up the unknown territory before making his next move.

For over sixty years now, Erdős has been the world's most celebrated problem solver and problem poser. unrivalled, king, non-pareille, ... He has been called an occidental Ramanujan, a modern-day Euler, the Mozart of mathematics. These glowing epithets accurately capture the different facets of Paul Erdős – each is correct in its own way. He has a unique talent to pose penetrating questions. It is easy to ask questions that lead nowhere, questions that are either impossibly hard or too easy. It is a completely different matter to raise, as Erdős does, innocent-looking problems whose solutions shed light on the shape of the mathematical landscape.

An important feature of the problems posed by Erdős is that they carry differing monetary rewards. Needless to say, this is done in jest, but the prizes do indicate Erdős's assessment of the difficulty of the problems. How different this is from the annoying habit of some mathematicians, who casually mention a problem as if they hadn't even thought about it, when in fact they are telling you the central problem they have been working on for a long time!

Two features of his mathematical *œuvre* stand out: his mastery of *elementary* methods and his advocacy of *random* methods. Starting with his very first papers, Erdős championed *elementary* methods in diverse branches of mathematics. He showed, again and again, that elementary methods often succeed against overwhelming odds. In many brilliant proofs he showed that, rather than bringing somewhat foreign machinery to bear on some problems,

and thereby trying to fit a square peg into a round hole, one can progress considerably further by facing the complications, going deep into the problem, and tailoring our approach to the intrinsic difficulties of the problem. This philosophy can pay unexpected dividends, as shown by Charles Read's solution of the Invariant Subspace Problem, Miklós Laczkovich's solution of Tarski's problem of "Squaring the Circle", and Tim Gowers' recent solutions of Banach's last unsolved problems, including the Hyperplane Problem.

As to *probabilistic* methods, by now it is widely acknowledged that these can be remarkably effective in tackling main-line questions in diverse areas of mathematics that have nothing to do with probability. It is worth remembering, though, that when Erdős started it all, the idea was very startling indeed. That today we take it in our stride is a sign of the tremendous success of the random method, which is very much his method, still frequently called the *Erdős method*.

Paul Erdős was born on 26th March 1913, in Budapest. His parents were teachers of mathematics and physics; his father translated a book on aircraft design from English into Hungarian. The young Paul did not go to elementary school, but was brought up by his devoted mother, Anna, and, for three years, between the ages of 3 and 6, he had a German *Fraulein*. His exceptional talent for mathematics was evident by the time he was three: his agility at mental arithmetic impressed all comers, and he was not yet four when he discovered negative numbers for himself. With the outbreak of the First World War, his father was drafted into the Austro-Hungarian army, and served on the Eastern Front. He was taken prisoner by the Russians, and sent to Siberia to a prisoner of war camp, from which he returned only after about six years.

After the unconditional surrender of Hungary at the end of the War, the elected government resigned, as it could not accept the terms of the Allies. These terms left Hungary only the rump of her territory, and in March 1919 the communists took over the country, with the explicit aim of repelling the Allies. The communists formed a *Dictatorship of the Proletariat*, usually referred to as the *Commune*, after its French equivalent in 1871, and set about defending the territory and forcibly reforming the social order.

The Commune could not resist the invasion by the Allies and the Hungarian "white" officers under *Admiral Horthy*, and it fell after a struggle of three months. Unfortunately for the Erdős family, Anna Erdős had a minor post under the Commune, and when Horthy came to power, she lost her job, never to teach again. Later she worked as a technical editor.

He studied elementary school privately with his mother. After that, in 1922, the young Erdős went to Tavaszmező gymnasium, the first year as a private pupil, the second and third years as a normal student, and the fourth year again as a private pupil. After the fourth year he attended St. Stephen's School (Szent István Gimnázium) where his father was a high school teacher. At this time Erdős also received significant instruction from his parents as

well. As it happened, my father entered the school just as Erdős left it, so they share many classmates, although they met only many years later.

By the early 1920s the *Mathematical Journal for Secondary Schools* (Középiskolai Matematikai Lapok) was a successful journal, catering for pupils with talent for mathematics. The journal had been founded in 1895 by a visionary young man, Dániel Arany, who hoped to raise the level of mathematics in the whole of Hungary by enticing students to mathematics through beautiful problems. The backbone of the journal was the year-long competition. Every month a number of problems were set for each age group; the readers were invited to submit their solutions, which were marked, and the best published under the names of the authors.

The young Erdős became an ardent reader of this journal, and his love of mathematics was greatly fanned by the intriguing problems in it. In some sense, Erdős's earliest publications date to this time, with the appearance of his solutions in the journal. On one occasion Paul Erdős and Paul Turán were the only ones who managed to solve a particular problem, and their solution was published under their joint names. This was Erdős's first "joint paper" with Turán, whom he had not even met at the time, and who later became one of his closest friends and most important collaborators.

Mathematicians, and especially young mathematicians, learn much from each other. Erdős was very lucky in this respect, for when at the age of 17 he entered the Pázmány Péter Tudományegyetem (the science university of Budapest) he found there an excellent group of about a dozen youngsters devoted to mathematics. Not surprisingly, Erdős became the focal point of this group, but the long mathematical discussions stimulated him greatly.

This little group included Paul Turán, the outstanding number theorist; Tibor Gallai, the excellent combinatorialist; Dezső Lázár, who was later tragically killed by the Nazis; George Szekeres and Esther Klein, who later married and subsequently emigrated to Australia; László Alpár, who became an important member of the Hungarian Mathematical Institute; Márta Svéd, another member of the group who went to live in Australia; and several others. Not only did they discuss mathematics at the university, but also in the afternoons and evenings, when they used to meet at various public places, especially by the *Statue of Anonymous*, commemorating the first chronicler of Hungarian history.

Two of Erdős's professors stand out: Lipót Fejér, the great analyst, and Dénes König, who introduced Erdős to graph theory. The lectures of König led to the first results of Erdős in graph theory: in answer to a question posed in the lectures, in 1931 he extended Menger's theorem to infinite graphs. Erdős never published his proof, but it was reproduced in König's classic, published in 1936.

As an undergraduate, Erdős worked mostly on number theory, obtaining several substantial results. He was not even twenty, when in Berlin the great Issai Schur lectured on Erdős's new proof of Bertrand's postulate. He

wrote his doctoral dissertation as a second year undergraduate, and it was not long before he got into correspondence with several mathematicians in England, including Louis Mordell, the great number theorist in Manchester, and Richard Rado and Harold Davenport in Cambridge. All three became Erdős's close friends.

When in 1934 Erdős finished university, he accepted Mordell's invitation to Manchester. He left Hungary for England in the autumn of 1934, not knowing that he would never again live in Hungary permanently. On 1st October 1934 he was met at the railway station in Cambridge by Davenport and Rado, who took him to Trinity College, and they immediately embarked on the first of their many long mathematical discussions. Next day Erdős met Hardy and Littlewood, the giants of English mathematics, before hurrying on to Mordell.

Mordell put together an amazing group of mathematicians in Manchester, and Erdős was delighted to join them. First he took up the *Bishop Harvey Goodwin Fellowship*, and was later awarded a *Royal Society Fellowship*. He was free to do research under Mordell's guidance, and he was soon producing papers with astonishing rapidity. In 1937 Davenport left Cambridge to join Mordell and Erdős, and their life-long friendship was soon cemented. I have a special reason to be grateful for the Erdős-Davenport friendship: many years later, I was directed to my present home, Trinity College, Cambridge, only because Davenport was a Fellow here, and he was a good friend of Erdős.

In 1938 Erdős was offered a fellowship at the Institute for Advanced Study in Princeton, so he soon thereafter sailed for the U.S., where he was to spend the next decade. The war years were rather hard on Erdős, as it was not easy to hear from his parents in Budapest, and when he received news, it was never good. His father died in August 1942, his mother later had to move to the Ghetto in Budapest, and his grandmother died in 1944. Many of his relatives were murdered by the Nazis.

In spite of being cut off from his home, Erdős continued to pour forth wonderful mathematics at a prodigious rate. Having arrived in America, he spent a year and a half at Princeton, before starting on his travels. He visited Philadelphia, Purdue, Notre Dame, Stanford, Syracuse, Johns Hopkins, to mention but a few places, and the pattern was set: like a Wandering Scholar of the Middle Ages, Erdős never stopped again. In addition to the many important papers he wrote by himself, he collaborated more and more with mathematicians from diverse areas, writing outstanding joint papers with Mark Kac, Wintner, Kai Lai Chung, Ivan Niven, Arye Dvoretzky, Shizuo Kakutani, Arthur A. Stone, Leon Alaoglu, Irving Kaplansky, Alfred Tarski, Gabor Szegő, William Feller, Fritz Herzog, George Piranian, and others. Through correspondence, he continued his collaboration with Paul Turán, Harold Davenport, Chao Ko and Tibor Gallai (Grünwald).

In 1954, he left the U.S. to attend the International Congress of Mathematicians in Amsterdam. He had also asked for a reentry permit at that

time but his request was denied. So he left without a reentry permit since in his own words, “Neither sam nor joe can restrict my right to travel.” Left without a country, Israel came to his aid, offering him employment at the Hebrew University in Jerusalem, and a passport. He arrived in Israel on 30th November 1954, and from then on he has been to Israel practically every year. Before leaving Israel for Europe in July 1955, he applied for a return visa to Israel. When the officials asked him whether he wanted to become an Israeli citizen, he politely refused, saying that he did not believe in citizenship.

After the upheaval following his trip to Amsterdam, he first returned to the U.S. in 1959; the relationship between Erdős and the U.S. Immigration Department was finally normalized in 1963, and since then he has had no problems with them.

In the *Treaty of Yalta*, Hungary was placed within the Soviet sphere of influence; the communists, aided by the Russians, took over the government, and turned Hungary into a *People’s Republic*. For ordinary Hungarians, leaving Hungary even for short trips to the West became very difficult. Nevertheless, in 1955 Erdős managed to return to Hungary for a short time, when his good friend, George Alexits, pulled strings and convinced the officials that, if Erdős were to enter the country, he should be allowed to leave.

Later Erdős could return to Hungary at frequent intervals, in order to spend more and more time with his mother, as well as to collaborate with a large number of Hungarian mathematicians, especially Turán and Rényi. In those dark days, Erdős was *the* main link between many Hungarian mathematicians and the West.

As a young pupil, I first heard him lecture during one of his visits: not only did he talk about fascinating problems but he also cut a flamboyant figure, with his suntan, Western suit and casual mention of countries I was sure I could never visit. I got to know him during his next visit: in 1958, having won the National Competition, I was summoned to the elegant hotel he stayed in with his mother. They could not have been kinder: Erdős told to me a host of intriguing questions, and did not talk down to me, while his mother (whom, as most of their friends, I learned to call *Annus Néni* or Aunt Anna) treated me to cakes, ice cream and drinks. Three years later they got to know my parents, and from then on they were frequent visitors to our house, especially for Sunday lunches. My father, who was a physician, looked after both Erdős and Annus Néni.

Seeing them together, there was no doubt that they were very happy in each other’s company: these were blissful days for both of them. Erdős thoroughly enjoyed being with his mother, and she was delighted to have her son back for a while. They looked after each other lovingly; each worried whether the other ate well and slept enough or, perhaps, was a little tired. Annus Néni was fiercely proud of her wonderful son, loved to see the many signs that her son was a great mathematician, and revelled in her role as the *Queen Mother of Mathematics*, surrounded by all the admirers and well-

wishers. She was never far from Erdős's mathematics either: she kept Erdős's hundreds of reprints in perfect order, sending people copies on demand.

Annus Néni was not young, having been born in 1880, but her health was good and she was very sharp. To compensate for the many years when they had been kept apart, Annus Néni started to travel with her son in her 80s; their first trip together being to Israel in November 1964. From then on they travelled much together: to England in 1965, many times to other European countries and the U.S., and towards the end of 1968 to Australia and Hawaii. When, tinged with envy, we told her that it must be wonderful to see the world, she replied "*You know that I don't travel because I like it but to be with my son.*" It was a tragedy for Erdős when, in 1971, Annus Néni died during a trip to Calgary. Her death devastated him and for years afterwards he was not quite himself. He still hasn't recovered from the blow, and it is most unlikely that he ever will.

Erdős's brushes with officialdom were not quite over: the communists also managed to upset him. In 1973 there was an international meeting in Hungary, to celebrate his 60th birthday. Erdős's friends from Israel were denied a visa to enter Hungary; this outraged him so much that for three years he did not return to Hungary.

With the collapse of communism and with the end of the Cold War, Erdős has entered a golden age of travel: not only can he go freely wherever he wants to, but he is even welcomed by officials everywhere.

Having started as a mathematical *prodigy*, by now Erdős is the *doyen* of mathematicians, with more friends in mathematics than the number of people most of us meet in a lifetime. As he likes to put it in his inimitable way, he has progressed from *prodigy* to *dotigy*. As a Member of the Hungarian Academy of Sciences, Erdős has a permanent position in Budapest. During summer months, he frequently stays in the Guest House of the Academy, two doors away from my mother, visiting Vera Sós, András Hajnal, Miklós Simonovits, András Sárközy, Miklós Laczkovich, and inspiring many others. Another permanent position awaits him in Memphis, where he stays and works with Ralph Faudree, and his other friends, Dick Schelp and Cecil Rousseau. In Israel he visits all the universities, including the Technion in Haifa, Tel Aviv, Jerusalem and the Weizman Institute. But for years now, Erdős has had many other permanent ports of call, including Kalamazoo, where Yousef Alavi looks after him; New Jersey and the New York area, where he stays with Ron Graham and Fan Chung and talks to many others as well, including János Pach, Joel Spencer, Mel Nathanson, Peter Winkler, Endre Szemerédi, Joseph Beck and Herb Wilf; Calgary, mostly because of Eric Milner, Richard Guy and Norbert Sauer; Atlanta, with Dick Duke, Vojtěch Rödl, Ron Gould and Dwight Duffus. And the list could go on and on, with Athens, Baton Rouge, Berlin, Bielefeld, Boca Raton, Bonn, Boston, Cambridge, Chicago, Los Angeles, Lyon, Minneapolis, Paris, Poznań, Prague, Urbana, Warsaw, Waterloo, and many others.

Honours have been heaped upon Erdős, although he could not care less. Every fifth year there is an International Conference in Cambridge on his birthday, and in 1991 Cambridge also awarded him a prestigious Honorary Doctorate, as did the Charles University of Prague a year later, and many other universities since. On the occasion of his 80th birthday, he was honoured at a spate of conferences, not only in Cambridge, but also in Kalamazoo, Boca Raton, Prague and Keszthely.

Nowadays Erdős lectures in more places than ever, interspersing his mathematical problems with stories about mathematicians and his remarks about life. He dislikes cold but, above all, hates old age and stupidity, and so he appreciates the languages in which these evils sound similar. Thus, *old* and *cold* and *alt* and *kalt* go hand in hand in English and German, and in no other language he knows. But Hindi is better still because the two greatest evils sound almost the same: *buddha* is old and *budu* is stupid.

Erdős is fond of paraphrasing poems, especially Hungarian poems, to illustrate various points. The great Hungarian poet at the beginning of this century, Endre Ady, wrote: *Legyen átkozott aki a helyembe áll!* (*Let him be cursed who takes my place!*) As a mathematician builds the work of others, so that his immortality depends on those who continue his work, Erdős professes the opposite: *Let him be blessed who takes my place!*

But Erdős does not wait for posterity to find people to continue his work: his extraordinary number of collaborators ensures that many people carry on his work all around the world. The collaborators who particularly stand out are Paul Turán, Harold Davenport, Richard Rado, Mark Kac, Alfréd Rényi, András Hajnal, András Sarközy, Vera Sós and Ron Graham: they have all done much major work with Erdős. In a moment we shall see a brief account of some of this work. Needless to say, our review of Erdős's mathematics will be woefully brief and inadequate, and will also reflect the taste of the reviewer.

Erdős wrote his first paper as a first-year undergraduate, on Bertrand's postulate that, *for every $n \geq 1$, there is a prime p satisfying $n < p \leq 2n$* . Bertrand's postulate was first proved by Chebyshev, but the original proof was rather involved, and in 1919 Ramanujan gave a considerably simpler proof of it. In his fundamental book, *Vorlesungen über Zahlentheorie*, published in Leipzig in 1927, Landau gave a rather simple proof of the assertion that for some $q > 1$ and every $n \geq 1$, there is a prime between n and qn . However, Landau's q could not be taken to be 2. In his first paper, Erdős sharpened Landau's argument, and by studying the prime factors of the binomial coefficient $\binom{2n}{n}$, gave a simple and elementary proof of Bertrand's postulate.

Erdős was quick to develop further the ideas in his first paper. In 1932, Breusch made use of L -functions to generalize Bertrand's postulate to the arithmetic progressions $3n + 1$, $3n + 2$, $4n + 1$ and $4n + 3$: for every $m \geq 7$ there are primes of the form $3n + 1$, $3n + 2$, $4n + 1$ and $4n + 3$ between m and $2m$.

By constructing expressions containing, as factors, all terms of the arithmetic progression at hand, and rather few other factors, Erdős managed to give an elementary proof of Breusch's theorem, together with various extensions of it to other arithmetic progressions. These results constituted the Ph.D. thesis Erdős wrote as a second-year undergraduate, and published in Sárospatak in 1934.

Schur, who had been Breusch's supervisor in Berlin, was quick to recognize the genius of the author of the beautiful elementary proof of Breusch's theorem. When, a little later, Erdős proved a conjecture of Schur on abundant numbers, and solved another problem of Schur, Erdős became "der Zauberer von Budapest" ("the magician of Budapest") – no small praise from the great German for a young man of twenty.

Abundant numbers figured prominently among the early problems tackled by Erdős. In his lectures on number theory, Schur conjectured that the abundant numbers have positive density: $\lim_{x \rightarrow \infty} A(x)/x$ exists, where $A(x)$ is the number of abundant numbers not exceeding x . (A natural number n is *abundant* if $\sigma(n)$, the sum of its positive divisors, is at least $2n$.) The beautiful elementary proof Erdős gave of this conjecture led him straight to other problems concerning the distribution of the values of real-valued additive arithmetical functions $f(n)$, that is functions $f : \mathbb{N} \rightarrow \mathbb{R}$ satisfying $f(ab) = f(a) + f(b)$ whenever $(a, b) = 1$.

These problems were first investigated by Hardy and Ramanujan in 1917, but were more or less forgotten for over a decade. As eventually proved by Erdős and Wintner in 1939, a real-valued additive arithmetical function $f(n)$ behaves rather well if the following three series are convergent:

$$\sum_{|f(p)| > 1} 1/p, \quad \sum_{|f(p)| \leq 1} f(p)/p \quad \text{and} \quad \sum_{|f(p)| \leq 1} f(p)^2/p,$$

with the summations over primes p . To be precise, the three series above are convergent if and only if $\lim_{x \rightarrow \infty} A_c(x)/x$ exists for every real c , where $A_c(x)$ stands for the number of natural numbers $n \leq x$ with $f(n) < c$.

In 1934, Turán gave a marvelous proof of an extension of the Hardy-Ramanujan theorem on the "typical number of divisors" of a natural number. Writing $\nu(n)$ for the number of *distinct* prime factors of n (so that $\nu(12) = 2$), Turán proved that

$$\sum_{n=1}^N \{\nu(n) - \log \log n\}^2 = N \log \log N + o(N \log \log N).$$

It is a little disappointing that Hardy, one of the greatest mathematicians alive, failed to recognize the immense significance of this new proof. Erdős, on the other hand, not only saw the significance of the paper, but was quick to make use of the probabilistic approach and so became instrumental in the birth of a very fruitful new branch of mathematics, *probabilistic number theory*. In a ground-breaking joint paper he wrote with Kac in 1939,

Erdős proved that if a bounded real-valued arithmetical function $f(n)$ satisfies $\sum_p f(p)^2/p = \infty$ then, for every $x \in \mathbb{R}$,

$$\lim_{m \rightarrow \infty} A_x(m)/m = \Phi(x),$$

where $A_x(m)$ is the number of positive integers $n \leq m$ satisfying

$$f(n) < \sum_{p \leq m} f(p)/p + x \left(\sum_{p \leq m} f(p)^2/p \right)^{1/2},$$

and, as usual

$$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-t^2/2} dt$$

is the *standard normal distribution*. In other words, the arithmetical function $f(n)$ satisfies the Gaussian law of error! It took the mathematical community quite a while to appreciate the significance and potential of results of this type.

Note that for $\nu(n)$, the number of prime factors of n , the Erdős-Kac theorem says that if $x \in \mathbb{R}$ is fixed then

$$\lim_{m \rightarrow \infty} \frac{1}{m} |\{n \leq m \text{ and } \nu(n) \leq \log \log m + x(\log \log m)^{1/2}\}| = \Phi(x).$$

Starting with his very first papers, Erdős championed “*elementary*” methods in number theory. That the number theorists in the 1930s appreciated elementary methods was due, to some extent, to Shnirelman’s great success in studying integer sequences, with a view of attacking, perhaps, the Goldbach conjecture. To study integer sequences, Shnirelman introduced a density, now bearing his name: an integer sequence $0 \leq a_1, < a_2 < \dots$ is said to have *Shnirelman density* α if

$$\inf_{x \geq 1} \frac{1}{x} \sum_{a_n \leq x} 1 = \alpha.$$

Thus if $a_1 > 1$ then the Shnirelman density of the sequence $(a_n)_{n=1}^{\infty}$ is 0.

Khintchine discovered the rather surprising fact that if $(a_n)_{n=1}^{\infty}$ is an integer sequence of Shnirelman density α with $0 < \alpha < 1$, and $(b_n)_{n=1}^{\infty}$ is the sequence of squares $0^2, 1^2, 2^2, \dots$, then the “sum-sequence” $(a_n + b_m)$ has Shnirelman density *strictly greater* than α . The original proof of this result, although elementary, was rather involved.

When Landau lectured on Khintchine’s theorem in 1935 in Cambridge, he presented a somewhat simplified proof he had found with Buchstab. Nevertheless, talking to Landau after his lecture, Erdős expressed his view that the proof should be considerably simpler and, to Landau’s astonishment, as soon as the next day he came up with a “proper” proof that was both elementary and short. In addition, the new proof also made it clear what the result had to do with squares: all one needs is that every positive integer is the sum of

at most four squares. If (b_n) is such that every positive integer is the sum of at most k terms b_n , then the sum-sequence $(a_n + b_m)$ has Shnirelman density at least $\alpha + \alpha(1 - \alpha)/2k$. It says much about Landau, that he immediately included this beautiful theorem of Erdős into the Cambridge “Tract” he was writing at the time (*Neue Ergebnisse der additiven Zahlentheorie*, published in 1937).

The difference between consecutive primes has attracted much attention. Writing p_n for the n^{th} prime, the *twin prime conjecture* states that $p_{n+1} - p_n$ is infinitely often equal to 2, that is $\liminf_{n \rightarrow \infty} (p_{n+1} - p_n) = 2$. At the moment we seem to be very far from a proof of this conjecture; in fact, there seems to be no hope to prove that $\liminf_{n \rightarrow \infty} (p_{n+1} - p_n) < \infty$. The *Prime Number Theorem*, asserting that $\pi(x) \sim x/\log x$, where $\pi(x)$ is the number of primes $p \leq x$, implies that $c = \liminf_{n \rightarrow \infty} (p_{n+1} - p_n)/\log p_n \leq 1$, but Erdős was the first to prove, in 1940, that $c < 1$. Later Rankin showed that $c \leq 59/60$, and then Selberg that $c \leq 15/16$. Subsequent improvements were obtained by Bombieri and Davenport and by Huxley; the present record, $c \leq 0.248$, is held by Maier.

Independently, Erdős and Ricci showed that the set of limit points of the sequence $(p_{n+1} - p_n)/\log p_n$ has positive Lebesgue density and yet, *no number is known to be a limit point*.

Concerning *large* gaps between consecutive primes, Backlund proved in 1929 that $\limsup_{n \rightarrow \infty} (p_{n+1} - p_n)/\log p_n \geq 2$. In quick succession, this was improved by Brauer and Zeitz (1930), by Westzynthius (1931), and then by Ricci (1934), to

$$\limsup_{n \rightarrow \infty} \frac{p_{n+1} - p_n}{\log p_n \log \log \log p_n} > 0.$$

By making use of the method of Brauer and Zeitz, Erdős proved in 1934 that

$$\limsup_{n \rightarrow \infty} \frac{(p_{n+1} - p_n)(\log \log \log p_n)^2}{\log p_n \log \log p_n} > 0.$$

In 1938 this result was improved by Rankin, who smuggled a factor $\log \log \log \log p_n$ into the denominator: there is a $c > 0$ such that

$$p_{n+1} - p_n > c \frac{\log p_n \log \log p_n \log \log \log \log p_n}{(\log \log \log p_n)^2} \quad (1)$$

for infinitely many values of n . It seems to be extremely difficult to improve this result, to the extent that Erdős is offering (according to him, perhaps a little rashly) \$10000 for a proof that (1) holds for every c . The original value of c given by Rankin was improved by Maier and Pomerance in 1990.

Although in the 1930s elementary methods were spectacularly successful in additive number theory and in the study of additive arithmetical functions, they did not seem to be suitable for the study of the distribution of primes. It was not only a desire for diverse proofs that urged mathematicians to search

for elementary proofs of results proved by deep analytical methods: many mathematicians, including Hardy, felt that if the *Prime Number Theorem* (PNT) could be proved by elementary methods then the *Riemann Hypothesis* itself might yield to a similar attack. This belief was reinforced by the result of Norbert Wiener in 1930 that the prime number theorem is *equivalent* to the fact that the zeta function $\zeta(s) = \zeta(\sigma + it)$ has no zero on the line $\sigma = 1$.

Next to the PNT, Dirichlet's classical theorem on primes in an arithmetical progression, proved in 1837, was a test case for the power of elementary methods. In 1948 Atle Selberg found an ingenious elementary proof of Dirichlet's theorem; indeed, Selberg proved that if k and l are relatively prime numbers then

$$\liminf_{x \rightarrow \infty} \frac{1}{\log x} \sum_{p \leq x; p \equiv l \pmod{k}} p^{-1} \log p > 0.$$

Shortly after this, Selberg proved the following *fundamental formula*:

$$\sum_{p \leq x} (\log p)^2 + \sum_{pq \leq x} \log p \log q = 2x \log x + O(x), \quad (2)$$

where p and q run over primes. This formula is an easy consequence of the PNT, but what caused the excitement was that Selberg gave a completely elementary proof. Thus the fundamental formula could be a starting point for elementary proofs of various theorems in number theory which previously seemed inaccessible by elementary methods.

Using Selberg's fundamental formula, Erdős quickly proved that $p_{n+1}/p_n \rightarrow 1$ as $n \rightarrow \infty$, where p_n is, as before, the n^{th} prime. Even more, Erdős proved (in an entirely elementary way) that if $c > 1$ then

$$\liminf_{x \rightarrow \infty} \frac{\log x}{x} (\pi(cx) - \pi(x)) > 0. \quad (3)$$

Erdős communicated this proof of (3) to Selberg, who, two days later, using (2), (3) and the ideas in the proof of (3), deduced the PNT $\lim_{x \rightarrow \infty} \frac{\pi(x) \log x}{x} = 1$. Thus an elementary proof of the PNT was found!

A little later Selberg found it possible to argue directly from (2), without making any use of (3); this is the way he wrote up his paper in the autumn of 1948. In a separate paper, Erdős stated (2), referred to Selberg's final proof of the PNT (not published at the time), gave his own proof of (3), Selberg's deduction of the PNT from (2) and (3), and a joint simplified deduction of the PNT from (2). In the *Mathematical Reviews* the great Cambridge mathematician A.E. Ingham found it convenient to review these two papers together. As he wrote, "All previous proofs have been by *transcendental*" arguments involving some appeal to the theory of functions of a complex variable. Successive proofs have moderated the demands on this theory, or invoked alternative analytical theories (e.g., Fourier transforms), but there remained a nucleus of complex variable theory, namely the proposition that

Riemann zeta-function $\zeta(s) = \zeta(\sigma + it)$ has no zeros on the line $\sigma = 1$; and this could hardly be avoided, except by a radically new approach, since the PNT is in a clearly definable sense “equivalent” to this property of $\zeta(s)$. It has long been recognized that an “elementary” proof of the PNT, not depending on analytical ideas remote from the problem itself, would (if indeed possible) constitute a discovery of the first importance for the logical structure of the theory of the distribution of primes. An elementary (though not easy) proof is given, in various forms, in these two papers.

“In principle, [the papers] open up the possibility of a new approach, in which the old logical arrangement is reversed and analytical properties of $\zeta(s)$ are deduced from arithmetical properties of the sequence of primes. How far the practical effects of this revolution of ideas penetrate into the structure of the subject, and how much of the theory will ultimately have to be rewritten, it is too early to say.”

For the startling elementary proof of the Prime Number Theorem Selberg was awarded a *Fields Medal*, and Erdős a *Cole Prize*, given every fourth year to the author of the best paper in algebra and number theory published in an American journal.

Let us say a few words about the contributions of Erdős to asymptotic formulae. One of the glorious achievements of the Hardy-Ramanujan partnership was the striking formula for $p(n)$, the number of different partitions of n (ignoring the order of the summands). By using powerful analytic methods that eventually led to the celebrated circle method of Hardy and Littlewood, in 1918 Hardy and Ramanujan gave an extremely good approximation for $p(n)$; later Rademacher improved the approximation a little and turned it into an *analytic expression* for $p(n)$. A weak form of the Hardy-Ramanujan result states that

$$p(n) \sim \frac{1}{4\sqrt{3}n} e^{\pi\sqrt{2n/3}},$$

and Hardy and Ramanujan also gave an elementary proof of

$$\log p(n) \sim \pi\sqrt{2n/3}.$$

Two decades later, Erdős set about proving that elementary methods can go considerably further, and in 1942 he proved that

$$p(n) \sim \frac{a}{n} e^{\pi\sqrt{2n/3}}$$

for some positive constant a .

Taking his cue from the Hardy-Ramanujan result mentioned a little earlier, that most integers n have about $\log \log n$ prime factors, Erdős also proved, with Lehner, that “almost all” partitions of a positive integer n contain about

$$A(n) = \frac{1}{\pi} \sqrt{3n/2} \log n$$

summands. Furthermore, there is also a beautiful distribution about $A(n)$: for $x \in \mathbb{R}$, the probability that a random partition of n has at most $A(n) + x\sqrt{n}$ summands tends to

$$e^{-\frac{\sqrt{6}}{\pi}e - \pi\sqrt{x/6}}.$$

Some years later, in 1946, Erdős returned to another variant of this problem. Given $n \in \mathbb{N}$, what is the *most likely* number of summands in a random partition of n ? Writing $k_0(n)$ for this number, it is not clear that $k_0(n)$ is well-defined although, as was shown later by Szekeres, this is the case. However, what does seem to be clear is that $k_0(n)$ is about $A(n)$. Erdős proved that, in fact,

$$k_0(n) = A(n) + \frac{\sqrt{6}}{\pi} \left(\log \frac{\sqrt{6}}{\pi} \right) \sqrt{n} + o(\sqrt{n}).$$

Another circle of problems that has occupied Erdős for over sixty years originated with a question raised by Sidon when Erdős and Turán went to see him. Given a sequence \mathcal{S} of natural numbers and $k \in \mathbb{N}$, write $r_k(n)$ for the number of representations of n in the form

$$n = a_1 + a_2 + \dots + a_k,$$

with $a_i \in \mathcal{S}$ and $1 \leq a_1 < a_2 < \dots < a_k$. Call \mathcal{S} an *asymptotic basis of order k* if $r_k(n) \geq 1$ whenever n is sufficiently large. In 1932 Sidon asked Erdős the following question. Is there an asymptotic basis of order 2 such that $r_2(n) = o(n^\epsilon)$ for every $\epsilon > 0$? The young Erdős confidently reassured Sidon that he would come up with such a sequence. Erdős was right, but it took him over twenty years: he proved in 1954 in Acta (Szeged) that for some constant c there is a sequence \mathcal{S} such that

$$1 \leq r_2(n) \leq c \log n$$

if n is large enough.

What can one say about $r_k(n)$ rather than $r_2(n)$? In 1990, Erdős and Tetali proved that for every $k \geq 2$ there are positive constants c_1, c_2 , and a sequence \mathcal{S} such that $c_1 \log n \leq r_k(n) \leq c_2 \log n$ if n is large enough. In fact, Erdős and Tetali gave two proofs of this theorem; the easier of the two gets the result as a fairly simple consequence of Janson's powerful and ingenious correlation inequality. The related conjecture of Erdős and Turán, made in 1941, that if $r_2(n) \geq 1$ for all sufficiently large n then $\limsup_{n \rightarrow \infty} r_2(n) = \infty$, is still far from being solved, although it seems possible that much more is true, namely if $r_2(n) \geq 1$ whenever n is large enough then $\limsup_{n \rightarrow \infty} r_2(n)/\log n > 0$.

In 1956, Erdős and Fuchs proved a remarkable theorem somewhat related to Sidon's problem but originating in a result of Hardy and Landau. Let us write $r(n)$ for the number of lattice points in \mathbb{Z}^2 in the circle of radius \sqrt{n} , so that $r(n)$ is the number of *integer* solutions of the inequality $x^2 + y^2 \leq n$. Gauss was the first to prove that $r(n)$ stays rather close to its expectation,

namely $r(n) - \pi n = O(n^{1/2})$. In 1906, Sierpiński returned to the study of $r(n)$, and showed that, in fact, $r(n) - \pi n = O(n^{1/3})$. The question whether this bound is essentially best possible or could be improved, intrigued many of the best number theorists in the first few decades of this century, including Hardy, Littlewood, Landau and Walfisz. In 1925 Hardy and Landau gave an exact expression for $r(n) - \pi n$ in terms of Bessel functions. They showed also that $r(n)$ does not stay too close to its expectation πn , namely that

$$\limsup_{n \rightarrow \infty} \frac{|r(n) - \pi n|}{(n \log n)^{1/4}} > 0.$$

Erdős and Fuchs, proved that this result has *nothing to do* with the sequence of squares $0^2, 1^2, \dots$ but it holds in great generality. Indeed, let $0 \leq a_1 \leq a_2 \leq \dots$ be any sequence of integers, and for $n \in \mathbb{N}$ let $r^*(n)$ be the number of solutions of the inequality $a_i + a_j \leq n$. Then, as proved by Erdős and Fuchs for *every positive real* α we have

$$\limsup_{n \rightarrow \infty} \frac{|r^*(n) - \alpha n|}{(n \log n)^{1/4}} > 0.$$

Erdős contributed much to the theory of diophantine approximation. Recall that a sequence $(\phi_n) \subset [0, 1]$ is said to be *uniformly distributed* if for all $0 \leq \alpha < \beta \leq 1$ we have

$$\lim_{n \rightarrow \infty} \frac{1}{n} \sum_{k \leq n, \alpha \leq \phi_k \leq \beta} 1 = \beta - \alpha. \quad (4)$$

Weyl proved in 1916 that $(\phi_n) \subset [0, 1]$ is uniformly distributed if, and only if,

$$\lim_{n \rightarrow \infty} \frac{1}{n} \sum_{j=1}^n e^{2\pi i k \phi_j} = 0$$

for every non-zero integer k . Needless to say, this necessary and sufficient condition gives no information about the speed in (4). To get some information about the speed of convergence, one needs a “finite” form of Weyl’s criterion. A finite form was given by van der Corput and Koksma in 1936, but a stronger conjecture of Koksma in his 1936 book on Diophantine approximation remained unproved until 1948, when Erdős and Turán proved the following remarkable theorem.

Let $\phi_1, \dots, \phi_n \in [0, 1]$, and set $s_k = \sum_{j=1}^n e^{2\pi i k \phi_j}$. Suppose that $|s_k| \leq \psi(k)$ for $k = 1, \dots, m$. Then for all $0 \leq \alpha < \beta \leq 1$ we have

$$\left| (\beta - \alpha)n - \sum_{\alpha \leq \phi_j \leq \beta} 1 \right| \leq C \left\{ \frac{n}{m} + \sum_{k=1}^m \psi(k)/k \right\}$$

for some absolute constant C .

This result has had numerous applications, starting with the following beautiful theorem from the original Erdős-Turán paper. For $n \geq 2$, let

$$f(z) = z^n + a_{n-1}z^{n-1} + \dots + a_1z + a_0 = \prod_{j=1}^n (z - z_j)$$

be such that $|z_j| \geq 1$ for every j . For $0 < \theta < 1$ set $M_\theta = \max_{|z|=\theta} |f(z)|$ and define $g(n, \theta)$, $2 \leq g(n, \theta) \leq n$, by

$$M_\theta / \sqrt{|a_0|} = e^{n/g(n, \theta)}.$$

Then for all $0 \leq \alpha < \beta \leq 2\pi$ we have

$$\left| \frac{\beta - \alpha}{2\pi} n - \sum_{\alpha \leq \arg z_j \leq \beta} 1 \right| < C \log(4/\theta) \frac{n}{\log g(n, \theta)},$$

where C is an absolute constant.

Note that if $M_\theta / \sqrt{|a_0|}$ is “not too large”, say at most $\epsilon\sqrt{n}$, then the error term above is $O(n/\log n)$.

Other applications were found by Egerváry and Turán, Környei, and others. When, in 1988, Laczkovich cracked Tarski’s fifty-year old problem on squaring the circle, he made substantial use of this theorem of Erdős and Turán from 1948.

There are very few people who have contributed more to the fundamental theorems in probability theory than Paul Erdős; here we shall state only a small fraction of the major results of Erdős in probability theory. The *law of the iterated logarithm* was proved around 1930 by Khintchine and Kolmogorov, with further contributions from Lévy. To state this fundamental result, let X_1, X_2, \dots be independent Bernoulli random variables, with $\mathbb{P}(X_n = -1) = \mathbb{P}(X_n = 1) = \frac{1}{2}$ for every n , and set $S_n = \sum_{i=1}^n X_i$. The law of the iterated logarithm states that $\limsup_{n \rightarrow \infty} S_n / \sqrt{2n \log \log n} = 1$ almost surely. Putting it another way, for $t \in [0, 1]$, let $t = 0.\epsilon_1(t)\epsilon_2(t)\dots$ be its dyadic expansion, or equivalently, set $\epsilon_n(t) = 0$ or 1 according as the integer part of 2^{nt} is even or odd. (Thus the variables $X_n(t) = 2\epsilon_n(t) - 1$ are as above.) Set $f_n(t) = \sum_{k=1}^n \epsilon_k(t) - \frac{n}{2}$. Then the law of iterated logarithm states that

$$\limsup_{n \rightarrow \infty} \frac{f_n(t)}{\left(\frac{n}{2} \log \log n\right)^{1/2}} = 1$$

for almost every $t \in [0, 1]$.

Let $\phi(n)$ be a monotone increasing non-negative function defined for all sufficiently large integers. Following Lévy, this function $\phi(n)$ is said to belong to the *upper class* if, for almost all t ,

$$f_n(t) \leq \phi(n)$$

provided n is sufficiently large, and it belongs to the *lower class* if, for almost all t , $f_n(t) > \phi(n)$ for infinitely many values of n . Then the law of the iterated logarithm states that $\phi(n) = (1 + \epsilon)(\frac{n}{2} \log \log n)^{1/2}$ belongs to the upper class if $\epsilon > 0$, and to the lower class if $\epsilon < 0$.

In 1942, Erdős considerably sharpened this assertion when he proved that a function

$$\left(\frac{n}{2 \log \log n}\right)^{1/2} \left\{ \log \log n + \frac{3}{4} \log_3 n + \frac{1}{2} \log_4 n + \dots + \frac{1}{2} \log_{k-1} n + \left(\frac{1}{2} + \epsilon\right) \log_k n \right\}$$

belongs to the upper class if $\epsilon > 0$, and to the lower class if $\epsilon < 0$. (We write \log_k for the k times iterated logarithm.) Not surprisingly, Erdős gave an elementary proof, and made no use of the results of Khintchine and Kolmogorov. Furthermore, as he indicated, the result could easily be extended to the case of Brownian motion. Some years later, Erdős returned to this topic in a joint paper with K.L. Chung.

In addition to the papers that were instrumental in creating *probabilistic number theory*, Erdős wrote some important papers with Mark Kac proving several basic results of *probability theory*. Let X_1, X_2, \dots, X_n be independent random variables, each with mean 0 and expectation 1. As before, set $S_k = \sum_{l=1}^k X_l$, $k = 1, \dots, n$. In 1946, Erdős and Kac determined the limiting distributions of $\max_{1 \leq k \leq n} S_k$ and $\max_{1 \leq k \leq n} |S_k|$, which turned out to be independent of the distribution of the X_i .

Although this result was important, the *method of proof* was even more so: Erdős and Kac proved that if the theorem can be established for one particular sequence of independent random variables satisfying the conditions of the theorem, then the conclusion of the theorem holds for *all* sequences of independent random variables satisfying the conditions of the theorem. Erdős and Kac called this the *invariance principle*. Since then, this principle has been widely applied in probability theory.

Erdős and Kac promptly proceeded to apply their powerful invariance principle to extending a beautiful result of Paul Lévy, proved in 1939. To state this result, let X_1, X_2, \dots be independent random variables, each with mean 0 and variance 1, such that the central limit theorem holds for the sequence. As before, let $S_k = X_1 + \dots + X_k$, and let N_n be the number of S_k , $1 \leq k \leq n$, which are positive. Erdős and Kac proved in 1947 that, in this case,

$$\lim_{n \rightarrow \infty} \mathbb{P}(N_n/n < x) = \frac{2}{\pi} \arcsin x^{1/2}$$

for all x , $0 \leq x \leq 1$. Thus N_n/n tends in distribution to the *arc sin distribution*.

What Paul Lévy had proved in 1939 is that this *arcsin law* holds in the binomial case $\mathbb{P}(X_k = 1) = \mathbb{P}(X_k = -1) = 1/2$.

In 1953 Erdős returned to this theme. In a joint paper with Hunt he proved that if X_1, X_2, \dots are independent zero-mean random variables with the same continuous distribution which is symmetric about 0 then, almost surely,

$$\lim_{n \rightarrow \infty} \frac{1}{\log n} \sum_{k=1}^n \frac{\text{sign } S_k}{k} = 0.$$

In his joint papers with Dvoretzky, Kac and Kakutani, Erdős contributed much to the theory of random walks and Brownian motion. For example, in 1940, Paul Lévy proved that almost all paths of a Brownian motion in the plane have double points. This was extended by Dvoretzky, Erdős and Kakutani in 1950: they proved that for $n \leq 3$ almost all paths of a Brownian motion in \mathbb{R}^n have double points, but for $n \geq 4$ almost all paths of a Brownian motion in \mathbb{R}^n are free of double points. In 1954, in a paper dedicated to Albert Einstein on his 75th birthday, Dvoretzky, Erdős and Kakutani returned to this topic, and proved that almost all paths of a Brownian motion in the plane have k -multiple points for every k , $k = 2, 3, \dots$; in fact, for almost all paths the set of k -multiple points is dense in the plane.

Let us say a few words about classical measure theory. A subset of a metric space is of *first category* if it is a countable union of nowhere dense sets. There are a good many striking similarities between the class of nullsets and the class of sets of first category *on the line*. Indeed, both are σ -ideals (i.e. σ -rings closed under taking subsets), both include all countable sets and contain some sets of cardinality c , both classes have power 2^c , both classes are invariant under translation, neither class contains an interval, in fact, the complement of any set of either class is a set dense in \mathbb{R} , the complement of any set of either class contains a member of the class with cardinality c , and so on.

Of course, neither class includes the other; also, it is easily seen that $\mathbb{R} = A \cup B$, with A of first category and B a nullset. Nevertheless, the existence of numerous common properties suggests that the two σ -ideals are *similar* in the sense that there is a one-to-one mapping $f : \mathbb{R} \rightarrow \mathbb{R}$ such that $f(E)$ is a nullset if and only if E is of first category. In 1934 Sierpiński proved that this is indeed the case, provided we assume the continuum hypothesis. Sierpiński went on to ask whether the stronger assertion is also true that, assuming the continuum hypothesis, there is a function *simultaneously* mapping the two classes into each other. In 1943 Erdős answered this question in the affirmative.

Assuming the continuum hypothesis, there is a one-to-one map $f : \mathbb{R} \rightarrow \mathbb{R}$ such that $f(E)$ is a nullset if and only if E is of first category, and $f(E)$ is of first category if and only if E is a nullset. In fact, f can be chosen to satisfy $f = f^{-1}$.

Of the many results of Erdős in approximation theory, let us mention some beautiful theorems concerning *Lagrange interpolation*. Let $X = \{x_{in}\}$, $n = 1, 2, \dots$, $i = 1, 2, \dots, n$, be a triangular matrix with

$$-1 \leq x_{1,n} < x_{2,n} < \dots < x_{n,n} \leq 1 \quad (5)$$

for every n . The values x_{in} are the *nodes* of interpolation. As usual, for $1 \leq k \leq n$, define the *fundamental polynomials* $l_{k,n}(x)$ as

$$l_{k,n}(x) = \prod_{i \neq k} (x - x_{i,n}) / \sum_{j=1}^n \prod_{i \neq j} (x_{k,n} - x_{i,n}).$$

so that $l_{k,n}(x)$ is the unique polynomial of degree $n - 1$ with zeros at $x_{i,n}$, $i \neq k$, with $l_{k,n}(x_{k,n}) = 1$.

The *Lebesgue functions* and the *Lebesgue constants* of the interpolation are

$$\lambda_n(x) = \sum_{k=1}^n |l_{k,n}(x)| \quad \text{and} \quad \lambda_n = \max_{-1 \leq x \leq 1} \lambda_n(x).$$

In fact, one frequently considers a generalization of the Lebesgue constants as well: for $-1 \leq a < b \leq 1$ set

$$\lambda_n(a, b) = \max_{a \leq x \leq b} \lambda_n(x),$$

so that $\lambda_n = \lambda_n(-1, 1)$.

Faber showed before the First World War that if X is any set of nodes satisfying (5) then $\lambda_n \geq \frac{1}{6} \log n$ for every n .

Much research was done on improving this inequality. After a series of papers with Turán, in 1942 Erdős proved the asymptotically best possible inequality that

$$\lambda_n > \frac{2}{\pi} \log n + O(1)$$

for every matrix X .

In 1931 Faber's inequality was extended by Bernstein, who proved that there is an absolute constant $c > 0$ such that

$$\lambda_n(a, b) \geq c \log n,$$

provided $-1 \leq a < b \leq 1$, and n is *sufficiently large, depending on (a, b)* . In other words, the L_∞ -norm of the restriction of $\lambda_n(x)$ to the interval (a, b) grows at least as fast as $c \log n$.

In a beautiful paper, written jointly with Szabados, Erdős proved in 1978 the *much stronger result* that a similar assertion holds for the *normalized L_1 -norms*.

There is an absolute constant $c > 0$ such that if X is an arbitrary system of nodes satisfying (5), $-1 \leq a < b \leq 1$, and n is sufficiently large, then

$$\int_a^b \lambda_n(x) dx \geq c(b - a) \log n.$$

In the special case $a = -1$, $b = 1$, the result had been announced by Erdős in 1961, but the proof in the Erdős-Szabados paper in 1978 was along different lines and simpler.

Let us turn to a substantial extension of some classical results of Faber and Bernstein. Given a system X of nodes satisfying (5), and a function F on $[-1, 1]$, let

$$L_n(F, X, x) = \sum_{k=1}^n F(x_{k,n}) l_{k,n}(x)$$

be the n^{th} Lagrange interpolation polynomial of F . Thus $L_n(F, X, x)$ is the unique polynomial of degree at most $n - 1$ whose value at $x_{k,n}$ is $F(x_{k,n})$, $1 \leq k \leq n$. Extending a result of Faber from 1914, Bernstein proved in 1931 that, for every triangular matrix X satisfying (5), there is a continuous function F and a point x_0 , $-1 \leq x_0 \leq 1$, such that

$$\limsup_{n \rightarrow \infty} |L_n(F, X, x_0)| = \infty. \quad (6)$$

In 1936, Géza Grünwald and Marcienkiewicz proved that if X is the “good” Chebyshev matrix then for some continuous function F relation (6) holds for almost every x_0 , and 1978 Privalov proved the same assertion for the class of Jacobi matrices.

After these results concerning special classes of matrices, in 1980 Erdős and Vértesi proved the striking result that a similar assertion holds for *every* matrix X satisfying (5): *there is always a continuous function F such that (6) holds for almost every x_0* . The proof is intricate and ingenious.

To conclude our brief list of results on approximation theory, let us return to an early major result of Erdős. It has been known since Newton that interpolation polynomials can be used to approximate definite integrals of functions. Indeed, as proved by Stieltjes, if the n^{th} row of X consists of the roots of the n^{th} Legendre polynomial then

$$\lim_{n \rightarrow \infty} \int_{-1}^1 L_n(F, X, x) dx = \int_{-1}^1 F(x) dx$$

for every Riemann integrable function F .

Later this result was extended to other matrices X formed by the zeros of polynomials that were orthogonal in $[-1, 1]$ with respect to a weight function of the form $(1 - x)^\alpha (1 + x)^\beta$ for some α and β . However, this was not known for any general class of weight functions; furthermore, the result of Stieltjes could not even be sharpened to

$$\lim_{n \rightarrow \infty} \int_{-1}^1 |L_n(F, X, x) - F(x)| dx = 1.$$

In 1937, Erdős and Turán solved both problems. Let $p(x) \geq M > 0$ be Riemann integrable over $[-1, 1]$, and let $\omega_0(x), \omega_1(x), \dots$ be orthogonal polynomials in $[-1, 1]$ with respect to $p(x)$, with $\omega_n(x)$ being a monic polynomial of degree n . Let A_n, B_n be constants with $B_n \leq 0$ such that

$$R_n(x) = \omega_n(x) + A_n\omega_{n-1}(x) + B_n\omega_{n-2}(x)$$

has n different roots in $[-1, 1]$, and let X be the set of nodes formed by the roots of the polynomials R_1, R_2, \dots . Erdős and Turán proved that in this case every Riemann integrable function $F(x)$ on $[-1, 1]$ satisfies

$$\lim_{n \rightarrow \infty} \int_{-1}^1 |L_n(F, X, x) - F(x)| dx = 0.$$

Much of Erdős's work in real analysis concerns so-called *Tauberian theorems*. The origin of these results is a theorem of Tauber stating that if $\sum a_n x^n \rightarrow s$ as $x \rightarrow 1-$, and $na_n \rightarrow 0$ as $n \rightarrow \infty$, then $\sum a_n$ is convergent (to sum s). Hence if $na_n \rightarrow 0$ and $\sum a_n$ is Cesàro summable then $\sum a_n$ is convergent. Soon after the turn of the century, Landau, Hardy and Littlewood founded a flourishing branch of analysis by making extensive use of deep results resembling this theorem of Tauber. These *Tauberian theorems* claim that if a series is summable with a certain method of summation and satisfies certain additional conditions then it is also summable with a weaker method of summation. For example, Hardy and Littlewood proved in 1911 that if $\sum a_n$ is Borel summable (i.e. $\lim_{x \rightarrow \infty} e^{-x} \sum s_n x^n / n!$ exists, where $s_n = a_1 + \dots + a_n$) and $\sqrt{n}a_n \rightarrow 0$ then $\sum a_n$ is convergent. The second part of the elementary proof of the PNT was, essentially, such a Tauberian theorem.

Shortly after the elementary proofs of the Prime Number Theorem were found, Erdős proved that the PNT can be deduced from Selberg's fundamental formula *alone*, without any reference to other properties of the sequence of primes. What Erdős needed was the following Tauberian theorem: if $a_n \geq 0$ and $\sum_{k=1}^n a_k (s_{n-k} + k) = n^2 + O(n)$ then $s_n = n + O(1)$. Here, as before, $s_n = a_1 + \dots + a_n$.

Hardy and Littlewood also considered *lacunary* series and proved, among others, that under certain lacunarity conditions Abel-summability implies summability. In 1943, Meyer-König proved a similar lacunarity theorem for Euler summability: if $\sum a_n$ is Euler summable (i.e. $\lim_{n \rightarrow \infty} 2^{-n} \sum_{k=0}^n \binom{n}{k} s_k$ exists) and $a_n = 0$ except if $n = n_i$, where $n_1 < n_2 < \dots$ satisfies $n_{i+1}/n_i \geq c > 1$, then $\sum a_n$ is convergent. Meyer-König went on to conjecture the much stronger assertion that instead of $n_{i+1}/n_i \geq c > 1$ it suffices to demand that $n_{i+1} - n_i > A\sqrt{n_i}$ for some $A > 0$. In 1952 Erdős came very close to proving this conjecture: he showed that the assertion is true if $A > 0$ is *sufficiently large*.

Another Tauberian theorem of Erdős, proved with Feller and Pollard in 1949, is important in the theory of Markov chains. Let p_0, p_1, \dots be non-negative, with $\sum p_k = 1$ and $\mu = \sum k p_k$, and suppose that $P(z) = \sum_0^\infty p_k z^k$ is not a power series in z^t for any integer $t > 1$. Then $|P(z)| < 1$ for $|z| < 1$; in particular, $(1 - P(z))^{-1}$ is analytic in $|z| < 1$, say

$$\frac{1}{1 - P(z)} = \sum_{k=0}^{\infty} u_k z^k .$$

The Erdős-Feller-Pollard Theorem states that $\lim_{k \rightarrow \infty} u_k = 1/\mu$ if $\mu < \infty$ and $u_k \rightarrow \infty$ if $\mu = \infty$. The theorem has important consequences in probability theory, and in 1951 de Bruijn and Erdős also used it to study recursion formulae.

In a beautiful paper written with Niven in 1948, Erdős extended a result relating the zeros of a complex polynomial to the zeros of its derivative. Among other results, Erdős and Niven proved that *if r_1, r_2, \dots, r_n are the zeros of a complex polynomial, and R_1, R_2, \dots, R_{n-1} are the zeros of its derivative then*

$$\frac{1}{n} \sum_{j=1}^n |z - r_j| \geq \frac{1}{n-1} \sum_{j=1}^{n-1} |z - R_j|$$

for every $z \in \mathbb{C}$, with equality if, and only if, all the zeros r_j are on a half-line emanating from z .

In a difficult paper written with Szegő in 1942, Erdős tackled a problem concerning real polynomials. Extending Markov's classical theorem that if a polynomial f of degree n satisfies $|f(x)| \leq 1$ for $-1 \leq x \leq 1$, then $|f'(x)| \leq n^2$ for $-1 \leq x \leq 1$, Schur proved in 1919 that *if f is a polynomial of degree n with $|f(x)| \leq 1$ for $-1 \leq x \leq 1$, then $|f'(x_0)| \leq \frac{1}{2}n^2$, provided $-1 \leq x_0 \leq 1$ and $f''(x_0) = 0$* . Writing m_n for the smallest constant that would do in the inequality above instead of $\frac{1}{2}$, Erdős and Szegő proved that for $n > 3$ the extremum $m_n n^2$ is attained for $x_0 = 1$ (or -1) and the so-called *Zolotarev polynomials*. This enabled Erdős and Szegő to determine $\lim_{n \rightarrow \infty} m_n$ as well (which turned out to be 0.3124...).

Whatever branch of mathematics Erdős works in, in spirit and attitude he is a *combinatorialist*: his strength is the hands-on approach, making use of ingenious elementary methods. Therefore it is not surprising that Erdős helped to shape 20th century combinatorics as no-one else: with his results, problems, and influence on people, much of combinatorics in this century owes its existence to Erdős.

One of the fundamental results in combinatorics is a theorem (to be precise, a pair of theorems) proved by F.P. Ramsey in 1930. Erdős was the first to realize the tremendous importance of this “super pigeon-hole principle”, and did much to turn *Ramsey's finite theorem* into *Ramsey theory*, a rich branch of combinatorics, as witnessed by the excellent monograph of *Graham, Rothschild and Spencer*. In a seminal paper written in 1935, Erdős and his co-author, George Szekeres, tackled the following beautiful problem of Esther Klein: can we find, for a given n , a number $N(n)$ such that from any set of N points in the plane it is possible to select n points forming a convex polygon? Erdős and Szekeres showed that the existence of $N(n)$ is an easy consequence of Ramsey's theorem for finite sets. In fact, they discovered Ramsey's theorem for themselves, and were told only later that they had

been beaten to it by Ramsey. It is remarkable that Ramsey, working in Cambridge, and Erdős and Szekeres, working in Budapest, arrived at the same result independently and in totally different ways, but within a few years of each other. As it happened, the proof given by Erdős and Szekeres is much simpler than the original, and it also gives much better upper bounds for the various *Ramsey numbers*. In particular, they proved that if $k, l \geq 2$ then

$$R(k, l) \leq \binom{k+l-2}{k-1},$$

where the Ramsey number $R(k, l)$ is the smallest value of n for which every graph of order n contains either a complete graph of order k or l independent vertices.

In view of the simplicity of the proof of the Erdős-Szekeres bound, it is amazing that over 50 years had to pass before the bound above was improved appreciably. In 1986 Rödl showed that there is a positive constant $c > 0$ such that

$$R(k, l) \leq \binom{k+l-2}{k-1} / \log^c(k+l),$$

and, simultaneously and independently, Thomason replaced the power of the logarithm by a power of $k+l$. To be precise, Thomason proved that

$$R(k, l) \leq k^{-1/2+A\sqrt{\log k}} \binom{k+l-2}{k-1}$$

for some absolute constant $A > 0$ and all k, l with $k \geq l \geq 2$.

Concerning the lower bounds for $R(k, l)$, especially $R(k, k)$, the situation seems to be even more peculiar. It is not even obvious that $R(k, k)$ is not bounded from above by a polynomial of k . Indeed, it was again Erdős, who gave, in 1947, the following lower bound: *if $\binom{n}{k} 2^{-\binom{k}{2}+1} < 1$ then $R(k, k) > n$* . Erdős's proof is remarkable for its simplicity and its influence on combinatorics. Although there are very few mathematicians who do not know this proof, we present it here, since it is delightful and brief. Consider the set of all $2^{\binom{n}{2}}$ graphs on $\{1, 2, \dots, n\}$. What is the average number of complete subgraphs of order k ? Since each of the $\binom{n}{k}$ possible complete subgraphs of order k is contained in $2^{\binom{n}{2}-\binom{k}{2}}$ of our graphs, the average is $\binom{n}{k} 2^{-\binom{k}{2}} < 1/2$. Similarly, the average number of complete subgraphs of order k in the *complements* of our graphs is also $\binom{n}{k} 2^{-\binom{k}{2}} < 1/2$. Consequently, there is some graph G on $\{1, 2, \dots, n\}$ such that neither G nor its complement \bar{G} contains a complete graph of order k . Hence $R(k, k) > n$, as claimed.

It took over three decades to improve this wonderfully simple lower bound: in 1977 Spencer showed that an immediate consequence of the Erdős-Lovász Local Lemma is that

$$R(k, k) \geq k 2^{k/2} \left(\frac{\sqrt{2}}{\epsilon} + o(1) \right),$$

which is only about a factor 2 improvement. Needless to say, the combinatorialists are eagerly awaiting a breakthrough that more or less eliminates the gap between the upper and lower bounds for $R(k, k)$, but judging by the speed of improvements on the original bounds of Erdős, we are in for a long wait.

Erdős did not fail to notice that the other theorem of Ramsey from 1930, concerning infinite sets, also had a tremendous potential. In the 1950s and 1960s, mostly with his two great collaborators, Rado and Hajnal, Erdős revolutionized combinatorial set theory.

Ramsey's theorem concerning infinite sets, in its simplest form, states that if G is an infinite graph then *either* G *or* its complement \bar{G} contains an infinite complete graph. While this is very elegant, in order to express more complicated results succinctly, it is convenient to rely on the Erdős-Rado *arrow notation*. Given cardinals r , a and b_γ , $\gamma \in \Gamma$, where Γ is an indexing set, the partition relation

$$a \rightarrow (b_\gamma)_{\gamma \in \Gamma}^r$$

is said to hold if, given any partition $\bigcup_{\gamma \in \Gamma} I_\gamma$ of the set $A^{(r)}$ of all subsets of cardinality r of a set A with $|A| = a$, there is a $\gamma \in \Gamma$ and a subset B_γ of A with $|B_\gamma| = b_\gamma$ such that $B_\gamma^{(r)} \subset I_\gamma$. The same notation is used to express the analogous assertion when some or all the symbols r , a and b_γ denote *order types* rather than cardinalities. If Γ is a small set then one tends to write out all the b_γ s.

Thus, in this notation, the infinite Ramsey theorem is that

$$\aleph_0 \rightarrow (\aleph_0, \aleph_0)^r$$

for every integer r , with $r = 2$ being the case of graphs.

In 1933, Sierpiński proved that there is a graph of cardinality 2^{\aleph_0} which has *neither* an uncountable complete graph *nor* an uncountable independent set:

$$2^{\aleph_0} \not\rightarrow (\aleph_1, \aleph_1)^2,$$

so the “natural” extension of Ramsey's theorem is false. Sierpiński's result says that one can partition the pairs of real numbers in such a way that every uncountable subset of \mathbb{R} contains a pair from both classes. This partition somewhat resembles a Bernstein subset of \mathbb{R} .

If we are happy with one of the classes being merely *countably infinite* then Ramsey's theorem extends to all cardinals. This was proved in 1941 by Dushnik and Miller for regular cardinals, and extended by Erdős to singular cardinals. Thus,

$$\kappa \rightarrow (\kappa, \aleph_0)^2.$$

In the language of graphs, this means that if a graph on κ vertices does not contain a complete subgraph on κ vertices then it contains an infinite independent set.

The Erdős-Rado collaboration on partition problems started in 1949. One of their first results is an attractive assertion concerning \mathbb{Q} , the set of rationals. *If G is a graph on \mathbb{Q} then either G or its complement \bar{G} contains a complete graph whose vertex set is dense in an interval.* Years later this was considerably extended by Galvin and Laver.

After a good many somewhat *ad hoc* results, in 1956 Erdős and Rado gave the first systematic treatment of “arrow relations” for cardinals; in their fundamental paper, “*A partition calculus in set theory*”, they set out to establish a ‘calculus’ of partitions. Among many other results, they proved that *if $\lambda \geq 2$ and $\rho \geq \aleph_0$ are cardinals then*

$$(\lambda^\rho)^+ \rightarrow ((\lambda^\rho)^+, (\rho^+)_\rho)^2,$$

but

$$\lambda^\rho \not\rightarrow ((\lambda \cdot \rho)^+, \rho^+)^2.$$

In the special case $\lambda = 2$ and $\rho = \aleph_0$, the last relation is precisely Sierpiński’s theorem.

In proving their positive results, Erdős and Rado used so called “*tree arguments*”, arguments resembling the usual proof of Ramsey’s infinite theorem, but relying on sequences of *transfinite length*. Another important ingredient is a *stepping-up lemma*, enabling one to deduce arrow relations about larger cardinals from similar relations about smaller ones. Thus the trivial relation $\aleph_1 \rightarrow (\aleph_1)_{\aleph_0}^1$ implies that

$$(2^{\aleph_0})^+ \rightarrow (\aleph_1)_{\aleph_0}^2.$$

In 1965, in a monumental paper “*Partition relations for cardinal numbers*”, running to over 100 pages, Erdős, Hajnal and Rado presented an almost complete theory of the partition relation above for cardinals, assuming the *generalized continuum hypothesis*. For years after its publication, its authors lovingly referred to their paper as GTP, the *Giant Triple Paper*.

In fact, Erdős had taken an interest in extensions of Ramsey’s theorem for infinite sets well before the Dushnik-Miller result appeared. In 1934, in a letter to Rado, he asked whether if we split the countable subsets of a set A of cardinality a into two classes then there is an infinite subset B of A , all of whose countable subsets are in the same class. In the arrow notation, does $a \rightarrow (\aleph_0, \aleph_0)^{\aleph_0}$ hold for some cardinal a ? Almost by return mail, Rado sent Erdős his counterexample (which is, by now, well known), constructed with the aid of the axiom of choice. Later this question led to the study of partitions restricted in some way, including the study of Borel and analytic partitions, and to many beautiful results of Galvin, Mathias, Prikry, Silver, and others.

The first results concerning partition relations for *ordinals* were also obtained in 1954. In November 1954, on his way to Israel, Erdős passed through Zürich. He told his good friend Specker that he was offering \$20 for a proof

or disproof of the conjecture of his with Rado that $\omega^2 \rightarrow (\omega^2, n)^2$. Within a few days, Specker sent Erdős a proof which is, by now, well known. Erdős had high hopes of building on Specker's proof to deduce that $\omega^n \rightarrow (\omega^n, 3)^2$ for every integer $n \geq 3$, but could prove only $\omega^{2n} \rightarrow (\omega^{n+1}, 4)^2$. A little later Specker produced an example showing that

$$\omega^n \not\rightarrow (\omega^n, 3)^2$$

for every integer $n \geq 3$.

Neither Specker's proof, nor his (counter)example worked for

$$\omega^\omega \rightarrow (\omega^\omega, 3)^2.$$

Erdős rated this problem so highly that eventually, in the late 1960s, he offered \$250 for a proof or counterexample. The prize was won by Chang in 1969 with a very complicated *proof*, which was later simplified by Milner and Jean Larson.

The remaining problems are far from being easy, and Erdős is now offering \$1000 for a complete characterization of the values of α and n for which

$$\omega^{\omega^\alpha} \rightarrow (\omega^{\omega^\alpha}, n)^2$$

holds.

The theory of partition relations for *ordinals* took off after Cohen introduced *forcing methods* and Jensen created his theory of the constructible universe. Not surprisingly, in many questions "independence reared its ugly head", as Erdős likes to say. In addition to Erdős, Hajnal and Rado, a host of excellent people working on combinatorial set theory contributed to the growth of the field, including Baumgartner, Galvin, Larson, Laver, Máté, Milner, Prikry and Shelah. An account of most results up to the early 1980s can be found in the excellent monograph "*Combinatorial Set Theory: Partition Relations for Cardinals*" by Erdős, Hajnal, Máté and Rado, published in 1984.

In 1940 Turán proved a beautiful result concerning graphs, vaguely related to Ramsey's theorem. *For $3 \leq r \leq n$, every graph of order n that has more edges than an $(r-1)$ -partite graph of order n contains a complete graph of order r .* It was once again Erdős who, with Turán, Gallai and others, showed that Turán's theorem is just the starting point of a large and lively branch of combinatorics, *extremal graph theory*. In order to formulate the quintessential problem of extremal graph theory, let us recall some notation. As usual, we write $|G|$ for the *order* (i.e. number of vertices) and $e(G)$ for the *size* (i.e. number of edges) of a graph G . Given graphs G and H , the expression $H \subset G$ means that H is a *subgraph* of G . Let F be a fixed graph, usually called the *forbidden graph*. Set

$$ex(n; F) = \max\{e(G) : |G| = n \text{ and } F \not\subset G\}.$$

and

$$EX(n; F) = \{G : |G| = n, e(G) = ex(n; F), \text{ and } F \not\subseteq G\}.$$

We call $ex(n; F)$ the *extremal function*, and $EX(n; F)$ the *set of extremal graphs* for the *forbidden graph* F . Then the basic problem of extremal graph theory is to determine, or at least estimate, $ex(n; F)$ for a given graph F and, at best, to determine $EX(n; F)$. From here it is but a short step to the problem of excluding several forbidden graphs, i.e. to the functions $ex(n; F_1, \dots, F_k)$ and $EX(n; F_1, \dots, F_k)$ for a finite family F_1, \dots, F_k of forbidden graphs.

Writing K_r for the complete graph of order r , and $T_k(n)$ for the unique k -partite graph of order n and maximal size (so that $T_k(n)$ is the *k-partite Turán graph* of order n), Turán proved, in fact, that $EX(n; K_r) = \{T_{r-1}(n)\}$, i.e. $T_{r-1}(n)$ is the *unique* extremal graph, and so $ex(n; K_r) = t_{r-1}(n)$, where $t_{r-1}(n) = e(T_{r-1}(n))$ is the size of $T_{r-1}(n)$.

As it happens, Erdős came very close to founding extremal graph theory *before* Turán proved his theorem: in 1938, in connection with sequences of integers no one of which divided the product of two others, proved that for a *quadrilateral* C^4 we have $ex(n; C^4) = O(n^{3/2})$. However, at the time Erdős failed to see the significance of problems of this type: one of the very few occasions when Erdős was “blind”.

Before we mention some of the important results of Erdős in extremal graph theory, let us remark that in 1970 (!) Erdős proved the following beautiful extension of Turán’s theorem (so the *rest of the world* had been blind). Let G be a graph without a K_r , with degree sequence $(d_i)_1^n$. Then there is an $(r-1)$ -partite graph G^* (which, a fortiori, contains no K_r either) with degree sequence $(d_i^*)_1^n$, such that $d_i \leq d_i^*$ for every i . In this theorem, the achievement is in the audacity of *stating* the result: once it is stated, the proof follows easily.

Erdős conjectured another extension of Turán’s theorem which was proved in 1981 by Bollobás and Thomason. The conjecture was sharpened by Bondy. Let $|G| = n$ and $e(G) > t_{r-1}(n)$. Then *every vertex x of maximal degree d in G is such that the neighbours span a subgraph with more than $t_{r-2}(d)$ edges*. In this instance it is also true that once the full assertion has been made, the proof is just about trivial; in fact, it is simply a minor variant of the proof of the previous theorem of Erdős.

It is fitting that the *fundamental theorem of extremal graph theory* is a result of Erdős, and his collaborator, Stone. Note that, by Turán’s theorem, the maximal size of a K_r -free graph of order n is about $\frac{r-2}{r-1} \binom{n}{2}$; in fact, trivially,

$$\frac{r-2}{r-1} \binom{n}{2} \leq t_r(n) \leq \frac{r-2}{r-1} \frac{n^2}{2}.$$

Writing, as usual, $K_r(t)$ for the *complete r -partite graph with t vertices in each class*, Erdős and Stone proved in 1946 that if $r \geq 2$, $t \geq 1$ and $\epsilon > 0$ are fixed and n is sufficiently large then *every graph of order n and size at least*

$\left(\frac{r-2}{r-1} + \epsilon\right) \binom{n}{2}$ contains a $K_r(t)$. In other words, *even ϵn^2 more edges* than can be found in a Turán graph *guarantee not only a K_r , but a “thick” K_r* , one in which every vertex has been replaced by a group of t vertices.

Prophetically, Erdős and Stone entitled their paper “*On the structure of linear*

graphs”; this is indeed the significance of the paper: it not only gives us much information about the *size* of extremal graphs, but it is also the starting point for the study of the *structure* of extremal graphs. If F is a non-empty r -chromatic graph, i.e. $\chi(F) = r \geq 2$, then, precisely by the definition of the chromatic number, F is not a subgraph of $T_{r-1}(n)$, so $ex(n; F) \geq t_{r-1}(n) \geq \frac{r-2}{r-1} \binom{n}{2}$. On the other hand, $F \subset K_r(t)$ if t is large enough (say, $t \geq |F|$), so if $\epsilon > 0$ and n is large enough then

$$ex(n; F) < \left(\frac{r-2}{r-1} + \epsilon\right) \binom{n}{2}.$$

In particular, if $\chi(F) = r \geq 2$ then

$$\lim_{n \rightarrow \infty} ex(n; F) / \binom{n}{2} = \frac{r-2}{r-1},$$

that is the asymptotic density of the extremal graphs with forbidden subgraph F is $(r-2)/(r-1)$. Needless to say, the same argument can be applied to the problem of forbidding any finite family of graphs: given graphs F_1, F_2, \dots, F_k , with $\min \chi(F_i) = r \geq 2$, we have

$$\lim_{n \rightarrow \infty} ex(n; F_1, \dots, F_k) / \binom{n}{2} = \frac{r-2}{r-1}.$$

Starting in 1966, in a series of important papers Erdős and Simonovits went considerably further than noticing this instant consequence of the Erdős-Stone theorem. Among other results, Erdős and Simonovits proved that if $G \in EX(n; F)$, with $\chi(F) = r \geq 2$, then G can be obtained from $T_{r-1}(n)$ by the addition and deletion of $o(n^2)$ edges. Later this was refined to several results concerning the *structure* of extremal graphs. Here is an example, showing how very close to a Turán graph an extremal graph has to be. Let F_1, \dots, F_k be fixed graphs, with $r = \min \chi(F_i)$, and suppose that F_1 has an r -colouring in which one of the colour classes contains t vertices. Let $G_n \in EX(n; F_1, \dots, F_k)$. Then, as $n \rightarrow \infty$,

(i) the minimal degree of G_n is $((r-2)/(r-1) + o(1))n$,

(ii) the vertices of G_n can be partitioned into $r-1$ classes such that each vertex is joined to at most as many vertices in its own class as in any other class,

(iii) for every $\epsilon > 0$ there are at most $c_\epsilon = c(\epsilon; F_1, \dots, F_k)$ vertices joined to at least ϵn vertices in their own class,

- (iv) *there are $0(n^{2-1/t})$ edges joining vertices in the same class,*
 (v) *each class has $n/(r-1) + O(n^{1-1/2t})$ vertices.*

Returning to the Erdős-Stone theorem itself, let us remark that Erdős and Stone also gave a bound for the speed of growth of t for which $K_r(t)$ is guaranteed to be a subgraph of every graph with n vertices and at least $((r-2)/(r-1) + \epsilon) \binom{n}{2}$ edges.

Let us write $t(n, r, \epsilon)$ for the maximal value of t that will do. Erdős and Stone proved that $t(n, r, \epsilon) \geq (\log_{r-1}(n))^{1-\delta}$ for fixed $r \geq 2$, $\epsilon > 0$ and $\delta > 0$, and large enough n , where $\log_k(n)$ is the k times iterated logarithm of n . They also thought it plausible though unproved that $\log_{r-1}(n)$ would be about the “best” value.

This assertion was conjectured in several subsequent papers by Erdős, so it was rather surprising when, in 1973, Erdős and Bollobás proved that, for fixed $r \geq 2$ and $0 < \epsilon < 1/(r-1)$ the correct *order* of $t(n, r, \epsilon)$ is, in fact, $\log n$.

A little later, in 1976, Erdős, Bollobás and Simonovits sharpened this result, and the dependence of the implicit constant on r and ϵ was finally settled by Chvátal and Szemerédi, who proved that *there are positive absolute constants c_1 and c_2 such that*

$$c_1 \frac{\log n}{\log(1/\epsilon)} \leq t(n, r, \epsilon) \leq c_2 \frac{\log n}{\log(1/\epsilon)}$$

whenever $r \geq 2$ and $0 < \epsilon < 1/(r-1)$.

For a bipartite graph F , the general Erdős-Stone theorem is not sensitive enough to provide non-trivial information about $ex(n; F)$, since all it tells us is that $ex(n; F) = o(n^2)$. It was, once again, Erdős, who proved several of the fundamental results about $ex(n; F)$ when F is bipartite. In particular, he proved with Gallai in 1959 that for a path P_l of length l we have

$$ex(n; P_l) \leq \frac{l-1}{2} n .$$

By taking vertex-disjoint unions of complete graphs of order l , we see that this inequality is, in fact, an equality whenever $l|n$. The determination of $ex(n; P_l)$ was completed by Faudree and Schelp in 1973.

Another ground-breaking result of Erdős concerns supersaturated graphs, i.e. graphs with *slightly* more edges than the extremal graph. An unpublished result of Rademacher from 1941 claims that a graph of order n with *more than* $\lfloor n^2/4 \rfloor = t_2(n)$ edges contains not only one triangle but at least $\lfloor n/2 \rfloor$ triangles. In 1962 Erdős extended this result considerably; he showed that for some constant $c > 0$ every graph with n vertices and $\lfloor n^2/4 \rfloor + k$ edges has at least $k \lfloor n/2 \rfloor$ triangles, provided $0 \leq k \leq cn$. Later, this led to a spate of related results by Erdős himself, Moon and Moser, Lovász and Simonovits, Bollobás and others.

Erdős, the problem-poser par excellence, could not fail to notice how much potential there is in combining Ramsey-type problems with Turán-type problems.

The extremal graph for K_r , namely the Turán graph $T_{r-1}(n)$, is *stable* in the sense that if a K_r -free graph G on n vertices has almost as many edges as $T_{r-1}(n)$, then G is rather similar to $T_{r-1}(n)$; in particular, it has a large independent set. Putting it another way, if G is K_r -free and does not have a large independent set then $e(G)$ is much smaller than $t_{r-1}(n)$.

This observation led Erdős and Sós to the prototype of *Ramsey-Turán problems*. Given a graph H and a natural number l , let $f(n; H, l)$ be the smallest integer m for which every graph of order n and size more than m either contains H as a subgraph, or has at least l independent vertices.

Erdős and Sós were especially interested in the case $H = K_r$ and $l = o(n)$, and so in the function

$$l(r) = \lim_{\epsilon \rightarrow 0} \lim_{n \rightarrow \infty} f(n; K_r, \lfloor \epsilon n \rfloor) / \binom{n}{2}.$$

It is easily seen that $l(3) = 0$, and in 1969 Erdős and Sós proved that $l(r) = (r-3)/(r-1)$ whenever $r \geq 3$ is odd.

The stumbling block in determining $l(r)$ for even values of r was the case $r = 4$. Szemerédi proved in 1972 that $f(4) \leq 1/4$, but it seemed likely that $f(4)$ is, in fact, 0. Thus it was somewhat of a surprise when in 1976 Erdős and Bollobás constructed a graph on a k -dimensional sphere that shows $f(4) = 1/4$. In fact, this graph is rather useful in a number of other questions as well; it would be desirable to construct an infinite family of graphs in this vein.

Erdős, Hajnal, Sós and Szemerédi completed the determination of $l(r)$ in 1983 when they showed that $l(r) = (3r-10)/(3r-4)$ whenever $r \geq 4$ is even. Note that the condition that our graph does not have more than $o(n)$ independent vertices, *does* force the graph to have considerably fewer edges: Turán's theorem tells us that without the condition on the independence number the limit would be $(r-2)/(r-1)$.

Erdős was still a young undergraduate, when he became interested in *extremal problems* concerning *set systems*. It all started with his fascination with *Sperner's theorem* on the maximal number of subsets of a finite set with no subset contained in another. Sperner proved in 1928 that if the ground set has n elements then the maximum is attained by the system of all $\lfloor n/2 \rfloor$ -subsets. Erdős was quick to appreciate the beauty and importance of this result, and throughout his career frequently returned to problems in this vein.

In 1939, Littlewood and Offord gave estimates of the number of real roots of a random polynomial of degree n for various probability spaces of polynomials. In the course of their work, they proved that for some constant $c > 0$, if z_1, z_2, \dots, z_n are complex numbers with $|z_i| \geq 1$ for each i , then of the 2^n sums of the form $\pm z_1 \pm z_2 \pm \dots \pm z_n$, no more than

$$cr2^n(\log n)n^{-1/2} \tag{7}$$

fall into a circle of radius r .

On seeing the result, Erdős noticed immediately the connection with Sperner's theorem, especially in the real case. In fact, Sperner's theorem implies the following best possible assertion. *If x_1, \dots, x_n are real numbers of modulus at least 1, then no more than $\binom{n}{\lfloor n/2 \rfloor}$ of the sums $\pm x_1 \pm x_2 \pm \dots \pm x_n$ fall in an open interval of length 2.* From here it was but a short step to show that the maximal number of sums that can fall in an open interval of length $2r$ is precisely the sum of the r largest binomial coefficients $\binom{n}{k}$.

Concerning the complex case, Erdős improved the Littlewood-Offord bound (7), to an *essentially* best possible bound, by removing the factor $\log n$. More importantly, Erdős conjectured that the Sperner-type bound holds not only for real numbers, as he noticed, but for vectors of norm at least 1 in a Hilbert space. This beautiful conjecture was proved 20 years later by Kleitman and, independently, by Katona. In 1970, Kleitman gave a strikingly elegant proof of the even stronger assertion that *if x_1, x_2, \dots, x_n are vectors of norm at least 1 in a normal space, then there are at most $\binom{n}{\lfloor n/2 \rfloor}$ sums of the form $\pm x_1 \pm x_2 \pm \dots \pm x_n$ such that any two of them are at a distance less than 2.*

With Offord, in 1956 Erdős tackled the original Littlewood-Offord problem concerning random polynomials. They concentrated on the class of 2^n polynomials of the form $f_n(x) = \pm x^n \pm x^{n-1} \pm \dots \pm 1$. Refining the result of Littlewood and Offord, they proved that, with the exception of $o((\log \log n)^{-1/3})2^n$ polynomials, the equations $f_n(x) = 0$ have

$$\frac{2}{\pi} \log n + o((\log n)^{2/3} \log \log n)$$

real roots.

Let us turn to some results concerning *hypergraphs*, the objects most frequently studied in the extremal theory of set systems. For a positive integer r , an *r -uniform hypergraph*, also called an *r -graph* or *r -uniform set system*, is a pair (X, \mathcal{A}) , where X is a set and \mathcal{A} is a subset of $X^{(r)}$, the set of all r -subsets of X . The *vertex set* of this hypergraph is X , and \mathcal{A} is the set of (*hyper*)*edges*. The vertex set is frequently taken to be $[n] = \{1, \dots, n\}$, and our hypergraph is often referred to as a “collection of r -subsets of $[n]$ ”. For $r = 2$ an r -graph is just a graph. Although r -graphs seem to be innocuous generalizations of graphs, they are much more mysterious than graphs.

The most influential paper of Erdős on hypergraphs, “*Intersection theorems for systems of finite sets*”, written jointly with Chao Ko and Richard Rado, has a rather curious history. The research that the paper reports on was done in 1938 in England. However, at the time there was rather little interest in pure combinatorics, and the authors went their different ways: Erdős went to Princeton, Chao Ko returned to China, and Rado stayed in England. As a result of this, the paper was published only in 1961.

In its simplest form, the celebrated Erdős-Ko-Rado theorem states the following. Let $\mathcal{A} \subset [n]^{(r)}$, that is let \mathcal{A} be a collection of r -subsets of the set $[n] = \{1, 2, \dots, n\}$. If $n \geq 2r$ and \mathcal{A} is intersecting, that is if $A \cap B \neq \emptyset$ whenever $A, B \in \mathcal{A}$, then $|\mathcal{A}| \leq \binom{n-1}{r-1}$. Taking $\mathcal{A} = \{A \in [n]^{(r)} : 1 \in A\}$, we see that the bound is best possible. This result has been the starting point of much research in combinatorics. By now there are a good many proofs of it, including a particularly ingenious and elegant proof found by Katona in 1972.

The more general Erdős-Ko-Rado theorem states that if $1 \leq t \leq r$, $\mathcal{A} \subset [n]^{(r)}$ and \mathcal{A} is t -intersecting, that is if $|A \cap B| \geq t$ whenever $A, B \in \mathcal{A}$, then $|\mathcal{A}| \leq \binom{n-t}{r-t}$, provided n is large enough, depending on r and t .

In the original paper it was proved that $n \geq t + (r-t)\binom{r}{t}^3$ will do. Once again, the bound on $|\mathcal{A}|$ is best possible, as shown by a collection of r -subsets containing a fixed t -set. But the bound on n given by Erdős, Ko and Rado is far from being best possible. For $i = 0, 1, \dots, r-t$, let

$$\mathcal{A}_i = \{A \in [n]^{(r)} : |A \cap [t+2i]| \geq t+i\}.$$

It is clear that each \mathcal{A}_i is a t -intersecting system, and it so happens that $|\mathcal{A}_1| > |\mathcal{A}_0|$ if $n < (t+1)(r-t+1)$. Thus the best we can hope for is that the Erdős-Ko-Rado bound $\binom{n-t}{r-t}$ holds whenever $n \geq (t+1)(r-t+1)$.

It took many years to prove that this is indeed the case. In 1976 Frankl came very close to proving it: he showed it for all t except the first few values, namely for all $t \geq 15$. Finally, by ingenious arguments involving vector spaces, Richard Wilson gave a complete (and self-contained) proof of it in 1984.

The Erdős-Ko-Rado theorem inspired so much research that in 1983 Deza and Frankl considered it appropriate to write a paper entitled “*The Erdős-Ko-Rado theorem – 22 years later*”.

The first Erdős-Rado paper that appeared in print, in 1950, contained their *canonical Ramsey theorem for r -graphs*, to be precise, for $\mathbb{N}^{(r)}$, the collection of r -subsets of \mathbb{N} . This is yet another Erdős paper which had much influence on the development of Ramsey theory, especially through the work of Graham, Leeb, Rothschild, Spencer, Nešetřil, Rödl, Deuber, Voigt and Prömel. To formulate this result, let $X \subset \mathbb{N}$ or, for that matter, let X be any ordered set, and let r be an integer. A partition of $X^{(r)}$ into some classes (finitely or infinitely many) is said to be *canonical* if there is a set $I \subset [r]$ such that two r -sets $A = (a_1, \dots, a_r)$, $B = (b_1, \dots, b_r) \in X^{(r)}$ belong to the same class if, and only if, $a_i = b_i$ for every $i \in I$. Here we assumed that $a_1 < \dots < a_r$ and $b_1 < \dots < b_r$. Thus in a canonical partition, A and B belong to the same class if, and only, for each $i \in I$, the i^{th} element of A is identical with the i^{th} element of B .

Note that if all we care about is whether two r -sets belong to the same class or not, then for every ordered set X with more than r elements, $X^{(r)}$ has precisely 2^r distinct canonical partitions, one for each subset I of $[r]$. If X is infinite then there is only one canonical partition with *finitely* many

classes: this is the canonical partition belonging to $I = \emptyset$, in which all r -sets belong to the same class.

The Erdős-Rado canonical Ramsey theorem claims that *if we partition $\mathbb{N}^{(r)}$ into any number of classes then there is always an infinite sequence of integers $x_1 < x_2 < \dots$ on which the partition is canonical.* If $\mathbb{N}^{(r)}$ is partitioned into only finitely many classes then, as it was just remarked, on $X = \{x_1, x_2, \dots\}$ the canonical distribution belongs to $I = \emptyset$, that is all r -sets of X belong to the same class. Thus Ramsey's theorem for infinite sets is an instant consequence of the Erdős-Rado result.

The canonical Ramsey theorem has attracted much attention: it has been extended to other settings many times over, notably by Erdős, Rado, Galvin, Taylor, Deuber, Graham, Voigt, Nešetřil and Rödl.

In 1952 Erdős and Rado gave a rather good upper bound for the Ramsey number $R^{(r)}(n, \dots, n)_k = R^{(r)}(n; k)$ concerning (r) -graphs: $R^{(r)}(n; k)$ is the minimal integer m such that if $[m]^{(r)}$ is partitioned into k classes then there is always a subset $N \in [m]^{(n)}$ all of whose r -sets are in the same class. Putting it slightly differently, $R^{(r)}(n; k)$ is the minimal integer m such that every k -colouring of the edges of a complete r -graph of order m contains a monochromatic complete r -graph of order n . Writing $\exp_s k$ for the s times iterated exponential so that $\exp_1 k = k$, $\exp_2 k = k^k$, and $\exp_3 k = k^{k^k}$, Erdős and Rado proved that

$$R^{(r)}(n; k)^{1/n} < \exp_{r-1} k .$$

Although this seems a rather generous bound, in their GTP, Erdős, Hajnal and Rado proved that for $r \geq 3$ we have

$$R^{(r)}(n; k)^{1/n} > \exp_{r-2} k .$$

Erdős believes that the right order is given by the upper bound.

An important question concerning hypergraphs is to what extent the Erdős-Stone theorem can be carried over to them. The density $d(G)$ of an r -graph $G = (X, \mathcal{A})$ of order n is

$$d(G) = |\mathcal{A}| / \binom{n}{r} ,$$

so that $0 \leq d(G) \leq 1$ for every hypergraph. Call $0 \leq \alpha < 1$ a *jump-value* for r -graphs if there is a $\beta = \beta_r(\alpha) > \alpha$ such that for every $\alpha' > \alpha$ and positive integer m there is an integer n such that every r -graph of order at least n and density at least α' contains a subgraph of order at least m and density at least β . An immediate consequence of the Erdős-Stone theorem is that *every* α in the range $0 \leq \alpha < 1$ is a jump-value.

In 1965 Erdős proved that, for every $r \geq 1$, 0 is a jump-value for r -graphs and, in fact, $\beta_r(0) = r!/r^r$ will do. This is because if $\alpha' > 0$, $m \geq 1$ and n is sufficiently large then every r -graph of order at least n and density at least

α' contains a $K_r^{(r)}(m)$, a complete r -partite r -graph with m vertices in each class. Clearly,

$$d(K_r^{(r)}(m)) = m^r / \binom{rm}{r} \sim \frac{r!}{r^r}.$$

This seems to indicate that every α , $0 \leq \alpha < 1$, is a jump-value for r -graphs for every $r \geq 3$ as well. Nevertheless, for years no progress was made with the problem so that, eventually, Erdős was tempted to offer \$1000 for a proof or disproof of this assertion. In 1984, Frankl and Rödl won the coveted prize when they showed that $1 - l^{-(r-1)}$ is *not* a jump-value for r -graphs if $r \geq 3$ and $l > 2r$. In spite of this beautiful result, we are *very far* from a complete characterization of jump-values.

The important topic of Δ -systems was also initiated by Erdős. A family of sets $\{A_\gamma\}_{\gamma \in \Gamma}$ is called a Δ -system if any two sets have precisely the same intersection, that is if the intersection of any two of them is $\bigcap_{\gamma \in \Gamma} A_\gamma$. Given cardinals n and p , let $f(n; p)$ be the maximal cardinal m for which every collection of m sets, each of size (at most) n , contains a Δ -system of size p . In 1960, Erdős and Rado determined $f(n; p)$ for infinite cardinals but found that surprising difficulties arise when n and p are finite. Even the case $p = 3$ seems very difficult, so that they could not resolve their conjecture that

$$f(n; 3) \leq c^n \tag{8}$$

for some constant c .

As Erdős and Rado pointed out, it is rather trivial that $f(n; 3) > 2^n$. Indeed, let \mathcal{A} be the collection of n -subsets of a $2n$ -set $\{x_1, \dots, x_n, y_1, \dots, y_n\}$ containing precisely one of x_i and y_i for each i . Then $|\mathcal{A}| = 2^n$ and \mathcal{A} does not contain a Δ -system on three sets.

Abbott and Hanson have improved this bound to $f(n; 3) > 10^{n/2}$, but due to the very slow progress with the upper bound, for years now Erdős has offered \$1000 for a proof or disproof of (8). Recently, Kostochka has made some progress with the problem when he proved that $f(n; 3) < n! \left(\frac{c \log \log n}{\log \log \log n} \right)^{-n}$.

Let us turn to a flourishing area of mathematics that was practically created by Erdős. This is the theory of *random graphs*, started by Erdős and then, a little later, founded by Erdős and Rényi.

Throughout his career, Erdős had a keen eye for problems likely to yield to either combinatorial or probabilistic attacks. Thus it is not surprising that he had such a tremendous success in combining *combinatorics and probability*.

At first, Erdős used random methods to tackle problems in main-stream graph theory. We have already mentioned the delightful probabilistic argument Erdős used in 1947 to give a lower bound for the Ramsey number $R(k, k)$. A little later, in 1959, a more difficult result was proved by Erdős by random methods: *for every $k \geq 3$ and $g \geq 3$ there is a graph of chromatic number k and girth g* . Earlier results in this vein had been proved by Tutte, Zykov, Kelly and Mycielski, but before this beautiful result of Erdős,

it had not even been known that such graphs exist for any $k \geq 6$. Later ingenious *constructions* were given by Lovász, Nešetřil and Rödl, but these constructions lead to considerably larger graphs than obtained by Erdős.

In a companion paper, published in 1961, Erdős turned to lower bounds for the Ramsey numbers $R(3, l)$, and proved by similar probabilistic arguments that $R(3, l) > c_0 l^2 / (\log l)^2$ for some positive constant c_0 . In 1968, Graver and Yackel gave a good upper bound for $R(3, l)$, which was improved, in 1972, by Yackel. As expected, further improvements were harder to come by. In 1980, Ajtai, Komlós and Szemerédi proved that $R(3, l) < c_1 l^2 / \log l$; the difficult proof was simplified a little later by Shearer. Very recently, J.H. Kim improved greatly the lower bound due to Erdős, and so now we know that the order of $R(3, l)$ is $l^2 / \log l$.

Almost simultaneously with his beautiful applications of random graphs to extremal problems, Erdős, with Rényi, embarked on a *systematic* study of random graphs. The first Erdős-Rényi paper on random graphs, in 1959, is about the connectedness of $G_{n, M}$, the random graph with vertex set $[n] = \{1, 2, \dots, n\}$, with M randomly chosen edges. Extending an unpublished result of Erdős and Whitney, they proved, among others, that if $c \in \mathbb{R}$ and $M = M(n) = \lfloor \frac{1}{2} n (\log n + c) \rfloor$ then

$$\lim_{n \rightarrow \infty} \mathbb{P}(G_{n, M} \text{ is connected}) = e^{-e^{-c}}.$$

This implies, in particular, that if $M = M(n) = \lfloor \frac{1}{2} n (\log n + \omega(n)) \rfloor$ then

$$\lim_{n \rightarrow \infty} \mathbb{P}(G_{n, M} \text{ is connected}) = \begin{cases} 0 & \text{if } \omega(n) \rightarrow -\infty, \\ e^{-e^{-c}} & \text{if } \omega(n) \rightarrow c \in \mathbb{R}, \\ 1 & \text{if } \omega(n) \rightarrow \infty. \end{cases}$$

The result is easy to remember if one notes that the “obstruction” to the connectedness of a random graph is the existence of isolated vertices: if $|\omega(n)|$ is not too large, say at most $\log \log n$, then $G_{n, M}$ is *very likely* to be connected if it has no isolated vertices (and if it does have isolated vertices then, a fortiori, it is disconnected).

By now, quite rightly, this is viewed as a rather simple result, but when it was proved, it was very surprising. To appreciate it, note that a graph of order n with as few as $n - 1$ edges *need not be disconnected*, and a graph of order n with as many as $(n - 1)(n - 2)/2$ edges *need not be connected*.

A little later, in 1960, in a monumental paper, entitled “*On the evolution of random graphs*”, Erdős and Rényi laid the foundation of the *theory of random graphs*. As earlier, they studied the random graphs $G_{n, M}$ with n labelled vertices and M random edges for large values of n , as M increased from 0 to $\binom{n}{2}$. They introduced basic concepts like “threshold function”, “sharp threshold function”, “typical graph”, “almost every graph”, and so on. An important message of the paper was that most monotone properties

of graphs appear rather suddenly. A property Q_n of graphs of order n is said to be *monotone increasing* if Q_n is closed under the addition of edges. Thus being connected, containing a triangle or having diameter at most five are all monotone increasing properties. Erdős and Rényi showed that for many a fundamental structural monotone increasing property Q_n there is a threshold function, that is a function $M^*(n)$ such that

$$\lim_{n \rightarrow \infty} \mathbb{P}(G_{n,M} \text{ has } Q_n) = \begin{cases} 0 & \text{if } M(n)/M^*(n) \rightarrow 0, \\ 1 & \text{if } M(n)/M^*(n) \rightarrow \infty. \end{cases}$$

Later it was noticed by Bollobás and Thomason that in this weak sense every monotone increasing property of set systems has a threshold function; recently a considerably deeper result has been proved by Friedgut and Kalai, which takes into account the automorphism group of the property, and so is much more relevant to properties of graphs.

The more technical part of the “*Evolution*” paper concerns cycles, trees, the number of components and, most importantly, the emergence of the *giant component*. Erdős and Rényi showed that if $M(n) = \lfloor cn \rfloor$ for some constant $c > 0$ then, with probability tending to 1, the largest component of $G_{n,M}$ is of order $\log n$ if $c < \frac{1}{2}$, it jumps to order $n^{2/3}$ if $c = \frac{1}{2}$, and it jumps again, this time right up to order n if $c > \frac{1}{2}$. Quite understandably, Erdős and Rényi considered this “double jump” to be one of the most striking features of random graphs.

By now, all this is well known, but in 1960 this was a striking discovery indeed. In fact, for over two decades not much was added to our knowledge of this *phase transition* or, as called by many a combinatorialist, the *emergence of the giant component*. The investigations were reopened in 1984 by the author of these lines with the main aim of deciding what happens around $M = \lfloor n/2 \rfloor$; in particular, what *scaling*, what *magnification* we should use to see the giant component growing continuously. It was shown, among others, that if $M = n/2 + s$ and $s = o(n)$ but slightly larger than $n^{2/3}$ then, with probability tending to 1, there is a unique largest component, with about $4s$ vertices, and the second largest component has no more than $(\log n)n^2/s^2$ vertices. Thus, in a rather large range, on average every new edge adds four new vertices to the giant component!

With this renewed attack on the phase transition the floodgates opened, and quite a few more precise studies of the behaviour of the components near the point of phase transition were published, notably by Stepanov (1988), Flajolet, Knuth and Pittel (1989), Łuczak (1990, 1991) and others. To cap it all, in 1993 Knuth, Pittel, Janson and Łuczak published a truly prodigious (over 120 pages) study, “*The birth of the giant component*”, giving very detailed information about the random graph $G_{n,M}$ near to its phase transition.

Erdős and Rényi also stated several problems concerning random graphs, thereby influencing the development of the subject. In 1966, they themselves

solved the problem of 1-factors: if n is even and $M = M(n) = \lfloor \frac{n}{2}(\log n + c) \rfloor$ then the probability that $G_{n,M}$ has a 1-factor tends to $e^{-e^{-c}}$ as $n \rightarrow \infty$; the “obstruction” is, once again, the existence of isolated vertices.

The *Hamilton cycle* problem was a much harder nut to crack. As a Hamiltonian graph is connected (and has minimal degree 2), it is rather trivial that if, with probability tending to 1, $G_{n,M}$ has a Hamilton cycle and if $M = M(n)$ is written as

$$M = M(n) = \frac{n}{2}(\log n + \log \log n + \omega(n)),$$

then we must have $\omega(n) \rightarrow \infty$. On the other hand, it is far from obvious that a “typical” $G_{n,M}$ is Hamiltonian, even if $M = \lfloor cn \log n \rfloor$ for some large constant c . This beautiful assertion was proved in 1976 by Pósa, making use of his celebrated lemma. Several more years passed, before Komlós and Szemerédi proved in 1983 that $\omega(n) \rightarrow \infty$ also suffices to ensure that a “typical” $G_{n,M}$ is Hamiltonian. A little later Bollobás proved a sharper, hitting time type result that had been conjectured by Erdős and Spencer, connecting Hamiltonicity with having minimal degree at least 2.

The *chromatic number* problem from the 1960 “*Evolution*” paper of Erdős and Rényi was the last to fall. In 1988 the author of this note proved that *picking one of the $2^{\binom{n}{2}}$ graphs on $[n]$ at random, with probability tending to 1, the chromatic number of the random graph is asymptotic to $\frac{\log 2}{2}n / \log n$. Earlier results had been obtained by Grimmett and McDiarmid, Bollobás and Erdős, Matula, Shamir and Spencer, and others, and subsequent refinements were proved by Frieze, Łuczak, McDiarmid and others.*

The tremendous success of the theory of random graphs in shedding light on a variety of combinatorial, structural problems concerning graphs foreshadows the use of random methods in other branches of mathematics. Graphs carry only a minimal structure so they are bound to yield to detailed statistical analysis. However, as we acquire more expertise in applying results of probability theory, we should be able to subject more complicated structures to statistical analysis. In keeping with this philosophy, having founded, with Rényi, the theory of random graphs, Erdős turned to “the theory of random groups” with another great collaborator, Paul Turán. In a series of seven substantial papers, published between 1965 and 1972, Erdős and Turán laid the foundations of *statistical group theory*.

For simplicity, let us consider the symmetric group S_n , and let π_n be a random element of S_n , with each of the $n!$ possibilities equally likely. Thus π_n is a *random permutation* of $[n] = \{1, 2, \dots, n\}$, and every function of π_n is a *random variable*. One of the simplest of these random variables is the *order* $O(\pi_n)$ of a permutation π_n .

Concerning $g(n) = \max_{\pi \in S_n} O(\pi)$, the maximal order of a permutation, it was already shown by Landau in 1909 that

$$\lim_{n \rightarrow \infty} \frac{\log g(n)}{\sqrt{n \log n}} = 1 .$$

Thus $O(\pi_n)$ is *always* small compared to the order of the group S_n , although it *can* be rather large!

In contrast, for a single cycle of length n has order n , although such cycles constitute a non-negligible fraction, namely a fraction $1/n$, of all possible permutations. What is then the order of most elements of S_n ?

As the starting point of their investigations, Erdős and Turán proved that for a “*typical*” permutation π_n , the order $O(\pi)$ is much smaller than the maximum $g(n) = \exp\{(n \log n)^{1/2}(1 + o(1))\}$, and much larger than n . In fact, if $\omega(n) \rightarrow \infty$ (arbitrarily slowly, as always) then

$$\lim_{n \rightarrow \infty} \mathbb{P}(|\log O(\pi_n) - \frac{1}{2} \log^2 n| \geq \omega(n) \log^{3/2} n) = 0.$$

Thus the “typical” order is about $\frac{1}{2} \log^2 n$.

Erdős and Turán went on to prove that, asymptotically, $O(\pi_n)$ has a *log-normal* distribution: as $n \rightarrow \infty$,

$$\sqrt{3}(\log O(\pi_n) - \frac{1}{2} \log^2 n) / \log^{3/2} n$$

tends, in distribution, to the standard normal distribution, i.e. if $x \in \mathbb{R}$ then

$$\lim_{n \rightarrow \infty} \mathbb{P} \left(\frac{\sqrt{3}(\log O(\pi_n) - \frac{1}{2} \log^2 n)}{\log^{3/2} n} < x \right) = \Phi(x).$$

Having established this central limit theorem, which by now is known as the *Erdős-Turán law*, they went on to study the number $W(n)$ of *different* values of $O(\pi_n)$. (Thus $W(n)$ is the number of non-isomorphic cyclic subgroups of S_n .) Erdős and Turán proved that

$$W(n) = \exp \left\{ \pi \sqrt{\frac{2n}{3 \log n}} + O \left(\frac{\sqrt{n} \log \log n}{\log n} \right) \right\},$$

and, with the exception of $o(W(n))$ values, all are of the form

$$\exp \left\{ (1 + o(1)) \frac{\sqrt{6} \log 2}{\pi} \sqrt{n \log n} \right\}.$$

In S_n there are $p(n)$ conjugacy classes, where $p(n)$ is the partition function mentioned earlier, and studied in detail by Hardy and Ramanujan. As the order of a permutation $\pi \in S_n$ depends only on its conjugacy class K , it is natural to ask what the distribution of $O(K)$ is if the $p(n)$ conjugacy classes are considered equiprobable. Here we have written $O(K)$ for the order of any permutation in K . Erdős and Turán proved that, with probability tending to 1,

$$O(K) = \exp((A_0 + o(1))\sqrt{n}),$$

where

$$A_0 = \frac{2\sqrt{6}}{\pi} \sum_{j \neq 0} \frac{(-1)^{j+1}}{3j^2 + j} \approx 1.81.$$

All these results are proved by hard analysis, using Tauberian theorems and contour integration, somewhat resembling the Hardy-Ramanujan analysis; there is no reference to soft analysis or general theorems in probability theory or group theory that would get round the hard work. Thus it is not surprising that, over the years, many of the results of Erdős and Turán have been given shorter, more probabilistic proofs, that lead to sharper results. In particular, the Erdős-Turán law was studied by Best in 1970, Bovey in 1980, Nicolas in 1985 and Arratia and Tavaré in 1992. To date, the last word on the topic is due to Barbour and Tavaré, who used the *Ewens sampling formula*, derived by Ewens in 1972 in the context of population genetics, to give a beautiful proof of the Erdős-Turán law with a sharp error estimate. It is fascinating that, in order to get a small error term, Barbour and Tavaré had to adjust slightly the approximating normal distribution:

$$\sup_x |\mathbb{P}[\{\frac{1}{3} \log^3 n\}^{-1/2} (\log O(\pi_n) - \frac{1}{2} \log^2 n + \log n \log \log n) \leq x] - \Phi(x)| = O((\log n)^{-1/2}).$$

Numerous other problems of statistical group theory have been studied, including the problem of *random generation*. Dixon proved in 1969 that almost all pairs of elements of S_n generate S_n or the alternating group A_n , and recently Kantor and Lubotzky proved analogues of this result for finite classical groups. Because of problems arising in computational Galois theory, one is also interested in a considerably stronger condition than mere generation. The elements x_1, \dots, x_m of a group G are said to generate G *invariably* if G is generated by y_1, \dots, y_m whenever y_i is conjugate to x_i for $i = 1, 2, \dots, m$. Dixon showed in 1992 that for some constant $c > 0$, with probability tending to 1, $c(\log n)^{1/2}$ randomly chosen permutations generate S_n invariably. In 1993 Luczak and Pyber, confirming a conjecture of McKay, proved that *for every $\epsilon > 0$ there is a constant $C = C(\epsilon)$ such that C random elements generate S_n with probability at least $1 - \epsilon$.*

Luczak and Pyber also proved a conjecture of Cameron; they showed that *the fraction of elements of S_n that belong to transitive subgroups other than S_n or A_n tends to 0 as $n \rightarrow \infty$.*

Needless to say, in spite of these powerful results, many important questions remain unanswered, indicating that statistical group theory is still in its infancy.

When writing about the contributions of Erdős to mathematics, it would be unforgivable not to emphasize the enormous influence he exerts through his uncountably many problems. At the International Congress of Mathematicians in Paris in 1900, David Hilbert emphasized with great eloquence the importance of problems for mathematics. “The clearness and ease of comprehension insisted on for a mathematical theory I should still more demand

for a mathematical problem, if it is to be perfect. For what is clear and easily comprehended attracts; the complicated repels us.”

For lack of space, we shall confine ourselves to one more of the problems of Erdős that have been solved, and to three particularly beautiful unsolved questions.

There is no doubt that the most difficult Erdős problem solved to date is the problem on arithmetic progressions. In 1927 van der Waerden proved the following conjecture of Baudet: *if the natural numbers are partitioned into two classes then at least one of the classes contains arbitrarily long arithmetic progressions*. Over the years, this beautiful Ramsey-type result has been the starting point of much research. Quite early on, in 1936, Erdős and Turán suspected that *partitioning* the integers is an overkill: it suffices to take a “large” set of integers. Thus they formulated the following conjecture: *if A is a set of natural numbers with positive upper density, that is, if*

$$\limsup_{n \rightarrow \infty} \frac{|A \cap [n]|}{n} > 0,$$

then A contains arbitrarily long arithmetic progressions.

Roth was the first to put a dent in this Erdős-Turán conjecture when, in 1952, he proved that A must contain arithmetic progressions of length 3. Length 4 was much harder: Szemerédi proved it only in 1969. Having warmed up on length 4, in 1974 Szemerédi proved the full conjecture; the long and difficult proof is a real *tour de force* of combinatorics. The story did not end there: in 1977 Fürstenberg gave another proof of Szemerédi’s theorem, using tools of ergodic theory; the methods of this proof and the new problems it naturally led to revolutionized ergodic theory.

Let us turn then to the three unsolved Erdős problems we promised. The first asks for a substantial extension of Szemerédi’s theorem. Let $a_1 < a_2 < \dots$ be a sequence of natural numbers such that $\sum 1/a_n = \infty$. Is it true then that the sequence contains arbitrarily long arithmetic progressions? It is not even known that Roth’s theorem holds in this case, i.e. that the sequence contains an arithmetic progression with three terms. If this is not enough to indicate that this problem is rather hard, it is worth noting that Erdős offers \$5000 for a solution. A rather special case of the conjecture would be that the *primes* contain arbitrarily long arithmetic progressions.

The last two are also rather old conjectures, but each carries “only” a \$500 price-tag. Let $f(n)$ be the minimal number of distinct distances determined by n distinct points in the plane. Erdős conjectured in 1946 that

$$f(n) > \frac{cn}{\sqrt{\log n}}$$

for some absolute constant $c > 0$. The lattice points show that, if true, this is best possible. Chung, Szemerédi and Trotter have proved that $f(n)$ is at least about $n^{4/5}$.

The third problem is from the 1961 paper of Erdős, Ko and Rado; it is, in fact, the last unsolved problem of that paper. (However, Ahlswede and Khachatrian have just announced a proof of the conjecture.)

Let \mathcal{A} be a 2-intersecting family of $2n$ -subsets of $[4n] = \{1, 2, \dots, 4n\}$. Thus if $A, B \in \mathcal{A}$ then $A, B \subset [4n]$, $|A| = |B| = 2n$, and $|A \cap B| \geq 2$. Then the Erdős-Ko-Rado conjecture states that

$$|\mathcal{A}| \leq \frac{1}{2} \binom{4n}{2n} - \frac{1}{2} \binom{2n}{n}^2.$$

It is easily seen that, if true, this inequality is best possible. Indeed, let \mathcal{A} be the collection of $2n$ -subsets of $[4n]$, containing at least $n + 1$ of the first $2n$ natural numbers. Then \mathcal{A} is clearly 2-intersecting, and for every $2n$ -subset A on $[4n]$, the system contains precisely one of A and its complement \bar{A} , unless A (and so \bar{A} as well) contains precisely n of the first $2n$ natural numbers.

It is widely known that vast amounts of thought and ingenuity are required in order to earn \$500 on an Erdős problem; even so, this problem may be far harder than its price-tag suggests.

Although this brief review does not come close to doing justice to the mathematics of Paul Erdős, it does indicate that he has enriched the mathematics of this century as very few others have. He has clearly earned a *mathematical Oscar for lifetime achievement*, several times over. May he continue to prove and conjecture for many years to come.

Added in proof.

Sadly, this was not to be. On 20 September 1996, while attending a mini-semester at the Banach Center in Warsaw, Professor Paul Erdős was killed by a massive heart attack. Although in the last year he started to show signs of aging, his death was premature and entirely unexpected.

We combinatorialists have just become orphans.

B.B.