BOLYAI SOCIETY
MATHEMATICAL STUDIES, 11

Paul Erdős and his Mathematics. I,
Budapest, 2002, pp. 537–547.

Statistical Properties of Partitions

J.-L. NICOLAS*

In this paper, I recall a few personal souvenirs of Paul Erdős, his way of life and his great way of doing mathematics.

1. Paul Erdős and France

Before speaking about mathematics, I would like to say a few words about Paul Erdős and France. I guess that his parents gave him a certain idea of France, as the country of liberty, of human rights and of Bastille day. I am not sure whether France is really that country, but I certainly wish it strongly. When he was young, he read French novelists and I remember that Paul mentioned to me that he had read Anatole France who, I am afraid, is no longer read nowadays.

He was very much interested in history. Thirteen hundred years ago, the Arabs invaded Europe through Spain and the south of France, and were stopped at the battle of Poitiers in 732. One of Paul's favourite questions was "how many people were killed in this battle"?

I do not know when he visited France for the first time. In the spring of 1963, he gave a talk in the Number Theory seminar in Paris (the so-called Delange–Pisot–Poitou seminar) with the title "Problèmes et résultats sur les nombres premiers". H. Delange attended this lecture, and he told me that, as usual, Paul offered money for his problems. Thinking that the problem

* Research partially supported by CNRS, Institut Girard Desargues, UMR 5028, and by French-Hungarian scientific cooperation, Balaton 98009.

would not be solved for a very long time, he offered \$ $10^{(10!)}$ for showing that a multiplicative function g such that $|g(n)| \le 1$ for all $n \ge 1$ has a mean value (i.e. the sequence $\frac{1}{n}\sum_{m\le n} g(m)$ has a limit). The problem was solved by Wirsing a few years later (cf. [33] and [9], vol. I, p. 254).

I exchanged my first letters with P. Erdős in 1967, I met him for the first time in Montreal in 1968, and for the first time in France in June 1970, when he was invited to Paris by C. Berge and the late M. P. Schutzenberger. Further, I met him with his mother in Nice, in September 1970, at the International Congress of Mathematicians where he was an invited lecturer. Since then, he spent at least two weeks a year in France mainly visiting Bordeaux, Limoges, Nancy, Grenoble, Marseille, Strasbourg, Lyon and Paris.

Paul enjoyed good food, and perhaps to thank us, he used to invite my wife and me to good restaurants. He was also curious about food, asking for instance "what is this soup made with"? He was especially fond of French cheese. For his last visit to Lyon, he flew from Zurich. I drove to the airport in the evening to pick him up. I asked him: Paul, have you eaten? He answered: yes, I ate in the plane, but if you have a little bit of cheese... And, at home, he ate some cheese with a cubic centimeter of wine.

Let us return to mathematics. Paul Erdős was well known as a problem poser and a problem solver and, because of this, he was not much appreciated by Bourbaki, though J. Dieudonné once said (cf. [7]): *"rien de ce que fait Erdős n'est facile; c'est toujours extrêmement astucieux"*[1]. In Sections 4 and 5, by means of two examples in the theory of partitions, I would like to show how deep his way of thinking was, and how the problems he posed were often just steps to reach a more general point of view.

2. $a_i + a_j$ IS NOT A SQUARE

In this Section, I would like to show with an example how P. Erdős used to work, how he was a link between mathematicians, bringing mathematical news from university to university all over the world.

In a lecture in Limoges in June 1980, Paul stated one of his problems (cf. [19], [15], p. 87, 107 and [13]): let $1 \le a_1 < a_2 < \cdots < a_k \le n$ be a sequence of integers with the property that $a_i + a_j$ is never a square for all

[1] Nothing that Erdős does is easy; it is always extremely ingenious.

$1 \le i \le j \le k$. How large can k be in terms of n? Further, he mentioned that, if you choose $a_i = 3i+1$, then $a_i + a_j \equiv 2 \pmod 3$ cannot be a square and so $k = k(n) \gtrsim n/3$. At that time, I was involved in the number of squares modulo n (see [28]), so I asked myself: "why 3"? Why not to try to replace 3 by a larger integer such that the number of residue classes which are squares is small? I asked J.-P. Massias to carry out a few calculations, and he found, modulo 32, 11 residue classes the sum of no two of which is a square (cf. [27]). As $\frac{11}{32} > \frac{1}{3}$, by choosing a_i in all these 11 residue classes, it was possible to improve the preceding result to $k \gtrsim 11n/32$.

The following day, Paul flew to New York to visit J. Lagarias and A. M. Odlyzko at Bell Labs. He told them the result of Massias, and they were able (cf. [24] and [25]) in the following weeks, to show that, in the modular case, $\frac{11}{32}$ is maximal, and, in the general case, that $k \lesssim .475n$.

P. Erdős was very interested in the evolution of his problem. In all the letters he sent me in the next months, a few lines were devoted to the subject. On July 11, he wrote: *"There was a meeting in 1977 or 78 in Fort Collins, Colorado on combinatorial analysis; the volume of the meeting will soon appear. In my paper there, I mention the conjecture $a_i+a_j \ne n^2$ implies $\sum_{a_i<x} 1 = (1+o(1))\frac{x}{3}$ which was disproved by Massias"*. Further, on July 23, he wrote: *"Have you heard anything more about the computation of Massias? It would now be essential to prove that if $1 \le a_1 < \cdots < a_k \le n$ and $a_i + a_j$ is never a square then $k < \left(\frac{1}{2} - c\right) n$ where c is an absolute constant (we can of course assume $n > n_0$). I do not think that this could be hard but for the moment I do not see the proof"*. Later, on September 18, he wrote *"I spoke to Graham in the phone. Odlyzko and Lagarias proved that if $a_1, a_2, \ldots, a_k$ are residues mod m so that $a_i + a_j \not\equiv r^2 \pmod m$ then $k \le \frac{11}{32}m$. Thus your colleague's counterexample is best possible. They have results in the non modular case too but this is not yet so sharp"*.

3. IT IS OBVIOUS BY SIEVE METHOD...

Paul Erdős had a very deep understanding of the sieve method. Even though I knew this to be so, I was always surprised when, in a discussion, he said *"this is obvious by sieve method"*, because it had not come to my mind, and moreover, I needed a couple of hours to see how it was "obvious".

Many of his papers used sieve methods, and I shall give here examples of four articles which later had a strong influence in number theory and which were emphasized during the Budapest conference, in July 1999, by C. Pomerance, B. Bollobás, P. D. T. A. Elliott, H. Maier and A. Hildebrand.

In [10] it is proved that there is a positive proportion of primes p such that all the prime factors of $p-1$ are smaller than p^α where α is a fixed real constant smaller than 1. This result is an essential ingredient in the proof of the existence of infinitely many Carmichael numbers (cf. [1]).

In [16], the famous Erdős–Kac theorem is proved, and we may learn from Elliott (cf. [9], vol. II, p. 24) how they proved it. M. Kac was giving a talk in Princeton, and Paul was in the audience. At some point, the lecturer said that he would be able to prove what has become the Erdős–Kac theorem, provided some specific property of the integers is true. Very suddenly, Paul realised that this specific property was "obvious by sieve method", and before the end of the talk, the proof was completed.

Let us denote by p_n the n-th prime. In [11], it is proved that

$$\underline{\lim}\frac{p_{n+1}-p_n}{\log p_n} < 1.$$

The best known upper bound for the left hand side is 0.25542 (cf. [26]).

Let $d(n)$ denote the number of divisors of n. In [14], it is said: *"Brun's method easily gives that, for infinitely many n's,*

$$c_1 < \frac{d(n)}{d(n+1)} < c_2$$

and, in fact, that the set of limit points of $\frac{d(n)}{d(n+1)}$ *contains intervals".* This is probably the most striking example of this Section. Ask any number theoretist, even one well aware of sieve methods, to prove the above assertion; he will spend a lot of time. For the motivation of the question, see [23], and the references in it.

4. The Theorem of Erdős–Lehner

Let us recall first that a partition of n is a representation of n as the sum of any number of integral parts where the order of the parts is irrelevant, so that we can write a partition (Π) of n

$$n = n_1 + n_2 + \ldots + n_k, \quad n_1 \geq n_2 \geq \ldots \geq n_k. \tag{Π}$$

The total number of partitions of n will be denoted by $p(n)$. By the circle method, Hardy and Ramanujan gave (cf. [22]) a very nice formula for $p(n)$ from which the following estimation can be deduced:

$$p(n) \sim \frac{1}{4n\sqrt{3}}e^{C\sqrt{n}}, \qquad n \to \infty \tag{1}$$

with

$$C = \pi\sqrt{\frac{2}{3}} = 2.565\ldots \tag{2}$$

The first paper of Paul Erdős about partitions seems to be [12], where an elementary proof of the asymptotic estimate (1) was given. At about the same time, he wrote with J. Lehner the paper [17], where they studied the statistical distribution of the number of parts in a random partition of n.

It is well known that the number $p(n,m)$ of partitions of n with at most m parts is equal to the number of partitions of n with parts at most m, and so the generating function is

$$\sum_{n=0}^{\infty} p(n,m)q^n = \prod_{k=1}^{m}\frac{1}{1-q^k}. \tag{3}$$

By Cauchy's formula, (3) yields

$$p(n,m) = \frac{1}{2i\pi}\int_C \frac{1}{z^{n+1}}\left(\prod_{k=1}^{m}\frac{1}{1-z^k}\right)dz \tag{4}$$

where C is a circle of center O and radius smaller than 1. It is possible to use (4) together with the saddle point method to study the behaviour of $p(n,m)$, and this was done later by Szekeres in [31] and [32] in a very precise way. But, in [17], the sieve method was used to prove

Theorem. *Let*

$$m = \frac{1}{C}\sqrt{n}\log n + x\sqrt{n}, \tag{5}$$

with C defined by (2). *We have, for any fixed x, when $n \to \infty$,*

$$\lim \frac{p(n,m)}{p(n)} = \exp\left(-\frac{2}{C}\exp\left(-\frac{C}{2}x\right)\right). \tag{6}$$

The sketch of the proof given in ([17]) runs as follows: the number of partitions of n containing a part equal to a is clearly $p(n-a)$, and so, to count the number of partitions with parts at most m, you have to take off the partitions of n containing $m+1$, $m+2$, ..., up to n, the total number of which is $\sum_{r=1}^{n-m} p\big(n-(m+r)\big)$. But, in so doing, we have subtracted the partitions containing two large parts, say $m+r_1$ and $m+r_2$, twice and the sieving process appears and yields the formula

$$p(n,m) = p(n) - S_1 + S_2 - S_3 + \cdots + (-1)^k S_k + \cdots \tag{7}$$

with

$$S_k = \sum_{\substack{0<r_1<r_2<\cdots<r_k \\ 1\le r_1+r_2+\cdots+r_k\le n-mk}} p\big(n-(m+r_1)-(m+r_2)-\cdots-(m+r_k)\big). \tag{8}$$

By using the Hardy–Ramanujan result (1), the sum S_k in (8) can be evaluated, and for the value of m given by (5), the following relation holds:

$$\frac{S_k}{p(n)} \sim \frac{1}{k!}\left(\frac{2}{C}\exp\left(-\frac{C}{2}x\right)\right)^k. \tag{9}$$

But, it is well known from V. Brun that, in the alternating sum (7), the partial sums are alternately above and below the total value. From this, it is not difficult to deduce from (7) and (8) that, for the value of m given by (5), the following estimate holds:

$$p(n,m) = p(n)\left(1+\sum_{k\ge1}(-1)^k\frac{S_k}{p(n)}\right) \sim p(n)\exp\left(-\frac{2}{C}\exp\left(-\frac{C}{2}x\right)\right) \tag{10}$$

and (6) is an equivalent form of (10).

The paper [17] with J. Lehner was written soon after Kac's lecture mentioned in the preceding Section and the publication of the Erdős–Kac Theorem [16]. Clearly, Erdős had in mind that the additive structure of a partition, made of parts, is, in some sense, similar to the multiplicative structure of an integer, made of primes, which explains the use of a sieve method to prove (6). In the long series of papers [21], written with P. Turán, this idea was extended to the symmetric group on n letters, in order to study the statistical structure of a permutation, made of cycles.

In August 1998, attending the International Congress of Mathematicians in Berlin, I was pleased to hear two talks mentioning statistical studies of algebraic structures. In the abstract of his lecture (cf. [30]), A. Shalev says: *"We survey recent progress, made using probabilistic methods, on several conjectures concerning finite groups"*. Further, in the introduction, he indicates: *"The roots of the subject lie in a series of 7 papers of Erdős and Turán..."* (precisely, the papers [21]). Also, the aim of the lecture [6] of P. Diaconis was to show an intimate connexion between different areas of mathematics, specially algebra and probability.

5. Practical Partitions

Let $A \subset \mathbb{N}$. We can consider partitions of n with parts in A. Let us call $p_A(n)$ the number of these partitions. In the paper [3], jointly written with P. Bateman, a necessary and sufficient condition on the set A is given such that the function $n \mapsto p_A(n)$ is non decreasing from a certain point on. These partition functions had already been considered, for example by Hardy and Ramanujan, for particular values of A (the set of squares, of primes,...) but, as far as I know, only to give an asymptotic estimation of $p_A(n)$ as n goes to infinity. The paper [3] seems to be the first one for which the mapping $A \mapsto p_A(n)$ was considered from another point of view.

In order to give an estimation of the number of fundamental invariants of binary forms of degree d, J. Dixmier needed to study partition theory, and he asked Erdős and myself to help him. This is explained in [8] and was the beginning of a fruitful collaboration between the three of us and A. Sárközy. Let $n = n_1 + n_2 + \ldots + n_k$ be a partition Π of n, and a an integer. The partition Π is said to represent a if a can be written as a subsum $n_{i_1} + n_{i_2} + \ldots + n_{i_r}$ of the parts of Π. One of the problems studied in [8] is to estimate, for $r \ge 2$, the number of partitions of rn which do not represent $n, 2n, \ldots, (r-1)n$.

A partition of n is said to be practical if it represents all integers between 0 and n. In [20], P. Erdős and M. Szalay proved that almost all partitions of n are practical (i.e. the number of non practical partitions of n is $o\big(p(n)\big)$ as $n \to \infty$). In [18] this problem is extended to $p_A(n)$, for many sets A, but a nice counterexample due to D. Hickerson shows a set $A \subset \mathbb{N}$ such that, for infinitely many n's, most of the partitions are non practical.

Let us say that two partitions Π and Π' of the same number n are equivalent if they represent the same integers or, in other words, if $E(\Pi) = E(\Pi')$ where $E(\Pi)$ is the set of integers represented by Π. Let us denote by $\widehat{p}(n)$ the number of equivalence classes that is to say the number of distinct sets $E(\Pi)$ when Π runs over the $p(n)$ partitions of n. From the above mentioned result of [20], $\widehat{p}(n) = o(p(n))$ follows, and it was a question of P. Erdős to find a better estimation of $\widehat{p}(n)$. A first answer was given in [29]. The best result is in [5] and [2]: for n large enough, one has

$$p(n)^{0.361} \leq \widehat{p}(n) \leq p(n)^{0.768} \tag{11}$$

During his last visit to Lyon in early April 1996, Paul was interested in the same question for partitions with parts in A and specially for binary partitions, and he asked M. Deléglise to build a table of $\widehat{p}_A(n)$, when $A = \{1, 2, 4, 8, 16, \dots\}$ is the set of the powers of 2. I should say that I was not very enthusiastic about this idea, and I guessed that, after solving the question for binary partitions, Paul would have asked: *"What can be said if A is the set of squares, or the set of k-th powers, or the set of... ?"*

When, in September, we learnt that Paul had left, we decided, with M. Deléglise to finish that work. From the table, it was then clear to us that, for the set A of binary partitions, $\widehat{p}_A(n)$ is exactly equal to $q_A(2,n)$, the number of partitions of n, with parts in A, and where each part occurs at most twice (cf. [5]); in other words the generating function of $q_A(2,n)$ is

$$\sum_{n=0}^{\infty} q_A(2,n) q^n = \prod_{a \in A} (1 + q^a + q^{2a}). \tag{12}$$

Further, it was easy to prove that, for any set A which is 2-stable (i.e. $x \in A \Rightarrow 2x \in A$) and for a given partition Π of n with parts in A, there is a partition Π' of n, with parts in A, equivalent to Π (i.e. representing the same integers) with the property that each part in Π' occurs at most twice. In other words, if A is 2-stable, we have

$$\widehat{p}_A(n) \leq q_A(2,n). \tag{13}$$

Paul would have liked this simple result; unfortunately he did not see it, but it convinced me even more, that, as M. Simonovits said, P. Erdős was often fortunate in choosing his examples: essentially, looking at the binary partitions (the only ones for which (13) is an equality) was the key to the problem.

Curiously, the generating series defined by (12) with $A = \{1, 2, 4, 8, \dots\}$ was also studied, from a completely different point of view, in [4], as I recently learnt from R. Canfield.

Another Paul's question was to determine the largest classes of partitions of n (when $A = \mathbb{N}$). Of course, it follows from [20] that the largest class is the class of practical partitions, that is, the partitions representing all possible integers. In a forthcoming paper with M. Szalay, we shall show that the second largest class represents all integers between 0 and n except 1 and $n-1$, and we shall also investigate the next most popular classes after these two.

REFERENCES

[1] W. R. Alford, A. Granville and C. Pomerance, There are infinitely many Carmichael numbers, *Ann. of Math.*, **139** (1994), 703–722.

[2] J.-C. Aval, On sets represented by partitions, *European J. Combinatorics*, **20** (1999), 317–320.

[3] P. Bateman and P. Erdős, Monotonicity of partition functions, *Mathematika*, **3** (1956), 1–14.

[4] N. J. Calkin and H. S. Wilf, Recounting the rationals, *The American Math. Monthly*, **107** (2000), 360–363.

[5] M. Deléglise, P. Erdős and J.-L. Nicolas, Sur les ensembles représentés par les partitions d'un entier n, *Discrete Math.*, Special volume dedicated to the memory of P. Erdős, **200** (1999), 27–48.

[6] P. Diaconis, From Shuffling Cards to Walking around the Building: An Introduction to Modern Markov Chain Theory, *Proc. of the International Congress of Mathematicians, Berlin 1998, Documenta Mathematica, Journal der Deutschen Mathematiker-Vereinigung*, vol. I, 187–204.

[7] J. Dieudonné, Mathématiques vides et significatives, in: *Penser les Mathématiques*, Seuil (Paris, 1982).

[8] J. Dixmier, P. Erdős and J.-L. Nicolas, Sur le nombre d'invariants fondamentaux des formes binaires, *C. R. Acad. Sci. Paris*, **305**, Série I (1987), 319–322.

[9] P. D. T. A. Elliott, *Probabilistic Number Theory, vol. I and II*, Springer-Verlag (1980).

[10] P. Erdős, On the normal number of prime factors of $p-1$ and some related problems concerning Euler's φ function, *Quart. J. Oxford*, **6** (1935), 205–213.

[11] P. Erdős, The difference of consecutive primes, *Duke Math. J.*, **6** (1940), 438–441.

[12] P. Erdős, On an elementary proof of some asymptotic formulas in the theory of partitions, *Annals of Mathematics*, **43** (1942), 437–450.

[13] P. Erdős and D. Silverman, Problem 1162, *Colloquium Math.*, **42** (1979), p. 399.

[14] P. Erdős, Some problems on number theory, *Publications Mathématiques d'Orsay*, **86-1** (1986), 53–67.

[15] P. Erdős and R. L. Graham, Old and new problems and results in combinatorial number theory, *Monogr. l'Enseignement Mathématique*, **28** (1980).

[16] P. Erdős and M. Kac, On the Gaussian law of errors in the theory of additive functions, *Proc. of the Nat. Acad. of Sci.*, **25** (1939), 206–207 and *Amer. J. Math.*, **62** (1940), 738–742.

[17] P. Erdős and J. Lehner, The distribution of the number of summands in the partitions of a positive integer, *Duke Math. J.*, 8 (1941), 335–345.

[18] P. Erdős and J.-L. Nicolas, On practical partitions, *Collectanea Math.*, **46** (1995), 57–76.

[19] P. Erdős and A. Sárközy, On differences and sums of integers II, *Bull. Soc. Math. Grèce*, **18** (1977), 204–223.

[20] P. Erdős and M. Szalay, On some problems of J. Dénes and P. Turán, in: *Studies in Pure Math., dedicated to the memory of P. Turán*, Editor P. Erdős, Budapest, 1983, 187–212.

[21] P. Erdős and P. Turán, On some problems of a statistical group theory, I to VII, *Z. Wahrscheinlichkeitstheorie und verw. Gebiete*, **4** (1965), 175–186; *Acta Math. Acad. Sci. Hungar.*, **18** (1967), 151–163; **18** (1967), 309–320; **19** (1968), 413–435; *Period. Math. Hungar.*, **1** (1971), 5–13; *J. Indian Math. Soc.*, **34** (1970–71), 175–192; *Period. Math. Hungar.*, **2** (1972), 149–163.

[22] G.H. Hardy and S. Ramanujan, Asymptotic formulae in combinatory analysis, *Proc. London Math. Soc., (2)*, **17** (1918), 75–115 and Collected Papers of Ramanujan, §36, 276–309.

[23] A. Hildebrand, The divisor function at consecutive integers, *Pacific J. of Math.*, **129** (1987), 307–319.

[24] J. C. Lagarias, A. M. Odlyzko and J. B. Shearer, On the density of sequences of integers the sum of no two of which is a square I. Arithmetic progressions. *J. Combin. Theory Ser. A*, **33** (1982), 167–185.

[25] J. C. Lagarias, A. M. Odlyzko and J. B. Shearer, On the density of sequences of integers the sum of no two of which is a square II. General sequences, *J. Combin. Theory Ser. A*, **34** (1983), 123–139.

[26] H. Maier, Small differences between prime numbers, *Michigan Math. J.*, **35** (1988), 323–344.

[27] J.-P. Massias, Sur les suites dont les sommes des termes 2 à 2 ne sont pas des carrés. *Publications du département de Mathématiques de Limoges*, 4 (1982), 54–57.

[28] J.-L. Nicolas, Être ou ne pas être un carré, in: *Dopo la parole*, a collection of not always serious papers for A. Lenstra's doctorate (Amsterdam, 1984).

[29] J.-L. Nicolas and A. Sárközy, On two partition problems, *Acta Math. Acad. Sci. Hungar.*, **77** (1997), 95–121.

[30] A. Shalev, Simple Groups, Permutation Groups, and Probability, in: *Proc. of the International Congress of Mathematicians, Berlin 1998, Documenta Mathematica, Journal der Deutschen Mathematiker-Vereinigung*, vol. II, 129–137.

[31] G. Szekeres, An asymptotic formula in the theory of partitions, *Quart. J. Oxford (2)*, **2** (1951), 85–108.

[32] G. Szekeres, Some asymptotic formulæ in the theory of partitions II, *Quart. J. Oxford (2)*, 4 (1953), 96–111.

[33] E. Wirsing, Das asymptotische Verhalten von Summen über multiplikative Funktionen II, *Acta Math. Acad. Sci. Hungar.*, **18** (1967), 411–467.

Jean-Louis Nicolas

Institut Girard Desargues
UMR n° 5028
Mathématiques, Bât. 101
Université Claude Bernard (Lyon 1)
F-69622 Villeurbanne cédex
France

e-mail: jlnicola@in2p3.fr