Astérisque

ADOLF HILDEBRAND

Recent progress in probabilistic number theory

Astérisque, tome 147-148 (1987), p. 95-106

<http://www.numdam.org/item?id=AST_1987__147-148__95_0>

Société Mathématique de France
Astérisque 147-148 (1987), p.95-106.

RECENT PROGRESS IN PROBABILISTIC NUMBER THEORY

Adolf HILDEBRAND

1. Introduction

Probabilistic number theory (in the sense of [3]) can be described as the study of additive and multiplicative arithmetic functions from a general point of view, with an emphasis on probabilistic methods. A function $f: \mathbb{N} \to \mathbb{C}$ is called additive(resp. multiplicative), if it satisfies $f(nm)=f(n)+f(m)$ (resp. $f(nm)=f(n)f(m)$), whenever n and m are coprime. Most of the classical number-theoretic functions fall into one of these categories: $\mu(n)$ (the Moebius function), $\phi(n)$ (the Euler phi function) and $d(n)$ (the divisor function) are multiplicative functions; $\Omega(n)$ and $\omega(n)$ (the number of prime factors of n counted with resp. without multiplicity) are additive functions.

The relevance of a general approach to additive and multiplicative functions lies in the fact that many interesting results on the mentioned familiar arithmetic functions depend essentially only on the additivity or multiplicativity of the function in question and not on its particular definition. For example, it has been known since the beginning of this century that the limit $\lim_{x \to \infty} \frac{1}{x} \sum_{n \le x} \mu(n)$ exists, a result which lies quite deep, since it is known to be equivalent to the prime number theorem. It turns out that here the only relevant property of the Moebius function is that of being a multiplicative function with values in $[-1,1]$. In fact, Wirsing [19] proved in 1967, that for every such function the limit $\lim_{x \to \infty} \frac{1}{x} \sum_{n \le x} f(n)$ exists.

Probabilistic number theory has been developped in the last three decades. While in some areas the theory has reached a satisfactory stage of development, there remain others, where the results obtained so far are only fragmentary. I want to focus here on recently achieved results and open problems in those latter areas. A survey of "classical" probabilistic number theory can

be found, for example, in [2].

2. The Turán-Kubilius inequality

In 1917, Hardy and Ramanujan [8] proved that if $\Psi(n)$ is any function tending to infinity, then

$$\omega(n) = \text{loglog } n + O(\Psi(n)\sqrt{\text{loglog } n})$$

holds for "almost all" integers n, i. e. for $n \in \mathbb{N} \setminus E$, where

$$\lim_{x \to \infty} \frac{1}{x} \sum_{\substack{n \le x \\ n \in E}} 1 = 0 .$$

In 1934, Turán [18] gave a new proof for this result by establishing the inequality

$$(1) \qquad \frac{1}{N} \sum_{n \le N} (\omega(n) - \text{loglog } N)^2 << \text{loglog } N .$$

The theorem of Hardy and Ramanujan follows from (1) by Tchebycheff's inequality, a familiar and very useful tool in probability theory. Turán's method greatly influenced the further develoment of probabilistic number theory. Besides being simpler than the method of Hardy and Ramanujan, it had the advantage that it can be applied in very general situations, since the inequality (1) can be easily generalized. This generalization has been carried out in full by Kubilius [14], who derived a version of (1), which is valid uniformly for all additive functions.

Turán-Kubilius inequality: Let

$$\text{Var}(f,N) = \frac{1}{N} \sum_{n \le N} \Big| f(n) - \frac{1}{N} \sum_{n \le N} f(n) \Big|^2 ,$$

$$B(f,N) = \Big(\sum_{p^m \le N} \frac{|f(p^m)|^2}{p^m} \Big)^{1/2} .$$

Then the inequality

(2) $$\mathrm{Var}(f,N) \leq c\, B^2(f,N)$$

holds for all additive functions f and all $N \geq 1$ with an absolute constant c.

Besides being of some interest for its own sake, this inequality proved to be an extremely useful tool in establishing deeper results on the distribution of the values of additive functions. The question therefore arises, whether and to what extent it is sharp. It turns out that for a large class of additive functions (2) is indeed best-possible in the sense that an inequality in the opposite direction (with a different constant) holds. However, this is not always the case: for the additive function $f(n)=\log n$, the left-hand side of (2) remains bounded, as $N \to \infty$, while the right-hand side behaves like $\log^2 N$.

Recently, Ruzsa [16] showed that by slightly modifying the expression on the right of (2), one can obtain an inequality, in which both sides are of the same order of magnitude.

Ruzsa's inequality: There exist positive constants c_1 and c_2, such that the inequality

$$\mathrm{Var}(f,N) \left\{ \begin{array}{l} \leq c_1 \\ \geq c_2 \end{array} \right\} \min_{\lambda \in \mathbb{C}} \left\{ B^2(f-\lambda \log, N) + |\lambda|^2 \right\}$$

holds for all additive functions f and all $N \geq 1$.

A problem, which has attracted some attention in the past few years, is that of determining the "optimal" constant in (2). Let

$$c_N = \sup \mathrm{Var}(f,N) B^{-2}(f,N) \quad ,$$

where the supremum is taken over all additive functions f, for which $B(f,N) \neq 0$. Kubilius devoted several papers to the problem of estimating c_N from above and below, and at the Oberwolfach meeting in 1980 he formulated the conjecture

$$\lim_{N \to \infty} c_N = 1.5 \quad .$$

Shortly afterwards, Montgomery proved this conjecture (cf. [15]). Thus 1.5 is "asymptotically" the optimal constant in (2), but this yields no information about the optimal value for c in (2), i. e. $\sup_{N \geq 1} c_N$. Numerical calculations carried out by Kubilius [15] show that $c_N < 1.5$ for small values of N, and thus suggest the following

Conjecture: (2) holds with $c = 1.5$.

3. Limit distributions for additive functions

In 1939, Erdös and Kac [6] refined the theorem of Hardy and Ramanujan quoted in the preceding section by proving

Theorem (Erdös-Kac): For every $t \in \mathbb{R}$,

$$\lim_{N \to \infty} \frac{1}{N} \#\{n \leq N: \frac{\omega(n) - \log\log N}{\sqrt{\log\log N}} \leq t \} = \Phi(t) ,$$

where

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

is the distribution function of the Gaussian distribution.

Kubilius [14] and Shapiro [17] independently generalized this result to a large class of additive functions.

Theorem (Kubilius, Shapiro): Let $f: \mathbb{N} \to \mathbb{R}$ be additive, not identically zero, and suppose that

$$(3) \qquad \sum_{\substack{p \leq N \\ |f(p)| > \varepsilon B(f,N)}} \frac{f^2(p)}{p} = o(B^2(f,N)) \quad (N \to \infty) \text{ for every } \varepsilon > 0 .$$

Then we have

$$(4) \qquad \lim_{N\to\infty} \frac{1}{N} \#\{n\leq N: \frac{f(n) - A(f,N)}{B(f,N)} \leq t\} = \Phi(t) \qquad (t \in \mathbb{R}),$$

where $B(f,N)$ is defined as in section 2 and

$$A(f,N) = \sum_{p^m \leq N} \frac{f(p^m)}{p^m} .$$

It has been conjectured by Shapiro [17], but still not proved, that the condition (3) is actually necessary for (4) to hold.

The theorem of Kubilius and Shapiro can be viewed as a central limit theorem for additive functions, with the condition (3) being the analogue of the Lindeberg condition in the probabilistic central limit theorem. There exist by now a number of other theorems of this type, which constitute analogues of well-known limit theorems in probability theory. Such "limit theorems for additive functions" form the core of classical probabilistic number theory and are extensively treated in the monographs of Kubilius [14] and Elliott [3]. Among the few open problems that are left in this area, the most attractive is perhaps the above mentioned conjecture of Shapiro concerning the necessity of the "Lindeberg condition" (3).

4. Mean value theorems for multiplicative functions

The main problem in the theory of multiplicative functions is to estimate or evaluate asymptotically the means $\frac{1}{x} \sum_{n\leq x} f(n)$ of a multiplicative function f. Results in this direction, so-called mean value theorems, are potentially important for the study of additive functions. In fact, by the characteristic function method the distribution of the values of an additive function $g(n)$ can be linked to the behavior in mean of the multiplicative functions $\exp(itg(n))$, $t \in \mathbb{R}$.

A central question is whether for a given multiplicative function or a given class of multiplicative functions the "mean value"

$$\lim_{x\to\infty} \frac{1}{x} \sum_{n\le x} f(n)$$

exists. This can be a quite non-trivial problem, as the example of the Moebius function shows. In 1961, Delange [1] characterized those multiplicative functions of modulus ≤ 1, which have a non-zero mean value. Wirsing [19] showed in 1967 that any real-valued multiplicative function of modulus ≤ 1 has a mean value. Shortly afterwards, Halász [7] devised a powerful analytic method, which enabled him to give a new and simpler proof for Wirsing's theorem and to generalize it to complex-valued multiplicative functions. Halász also obtained quantitative mean value estimates, which had important applications in the theory of additive functions.

Recently, the author [9] derived Wirsing's mean value theorem from a large sieve inequality, a well-known and useful tool in analytic number theory. This method had the advantage that it can easily be adapted to deal with sums of multiplicative functions over short intervals. In particular, it yields the following short interval mean value theorem, which is the first of its kind.

Theorem [10]: *For any real-valued multiplicative function f of modulus ≤ 1 and any function $\Phi(x)\le x$ satisfying $\log\Phi(x)\sim \log x$ $(x\to\infty)$, the limit*

$$\lim_{x\to\infty} \frac{1}{\Phi(x)} \sum_{x-\Phi(x)<n\le x} f(n)$$

exists.

An interesting, but probably very difficult problem is to determine the behavior of multiplicative functions on special sequences such as the sequence of the values of a polynomial with integer coefficients at integers or at primes. Almost nothing is known in this direction. In particular, it has not yet been proved that the limits

$$\lim_{x\to\infty} \frac{1}{x} \sum_{n\le x} \mu(n^2+1) \quad , \quad \lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p\le x} \mu(p+1)$$

exist and are zero, as one would expect.

To conclude this section, I want to mention an old and very intriguing conjecture due to Erdös:

Conjecture: Let f be a completely multiplicative function (i. e. satisfying $f(nm)=f(n)f(m)$ for all $n,m \in \mathbb{N}$), assuming only the values ± 1. Then

$$\sup_{x \geq 1} \left| \sum_{n \leq x} f(n) \right| = \infty \quad .$$

5. Additive functions at consecutive integers

In 1946, Erdös [5] proved that a real-valued additive function f satisfying

$$f(n+1) - f(n) = o(1) \quad (n \to \infty) \tag{5}$$

or

$$f(n+1) \geq f(n) \quad (n \geq 1) \tag{6}$$

must be of the form

$$f = \lambda \log \tag{7}$$

for some $\lambda \in \mathbb{R}$. Wirsing [20] and Katai [12] independently showed that the first of these conditions can be weakened to

$$\lim_{x \to \infty} \frac{1}{x} \sum_{n \leq x} |f(n+1) - f(n)| = 0 \quad .$$

In 1979, Wirsing [21] proved that for a completely additive function the condition

$$f(n+1) - f(n) = o(\log n) \quad (n \to \infty)$$

already implies that f is a multiple of the logarithm.

These results show that, in a sense, the logarithm is the only "smooth" additive function. Very mild regularity conditions on the behavior of f (more specifically, on the behavior of the differences $f(n+1)-f(n)$) already imply that f is a multiple

of the logarithm.

The mentioned results are all of asymptotic nature. It is much more difficult to obtain quantitative estimates, which relate the behavior of the differences $f(n+1)-f(n)$ on a finite interval to that of $f(n)-\lambda \log n$ with a suitable λ on another finite interval. Elliott [4, Theorem 14.1] recently proved such a result, which had been previously conjectured by Ruzsa.

Theorem (Elliott): There exists an absolute constant c such that the inequality

$$\inf_{\lambda \in \mathbb{R}} \max_{n \le N} |f(n)-\lambda \log n| \le c \max_{n \le N^c} |f(n+1)-f(n)|$$

holds for all additive functions $f: \mathbb{N} \to \mathbb{R}$ and all $N \ge 1$.

This is a very powerful theorem, and it implies, often in a much stronger form, almost all previously known results in this area. For example, an immediate consequence of Elliott's theorem is that for any additive function $f: \mathbb{N} \to \mathbb{R}$ and any $\alpha \ge 1$ the estimate $f(n+1)-f(n)=O((\log n)^{\alpha})$ implies $f(n)=O((\log n)^{\alpha})$. Previously, this was only known when $1 \le \alpha \le 6/5$ or $\alpha \ge 3$ ([21], [22]).

The proof of Elliott's theorem is extremely complicated and takes up a large part of the book [4]. It involves many new ideas, some of which are of independent interest. A major role in the proof is played by a Bombieri-Vinogradov type theorem for additive functions.

Elliott in fact proved a more general result, involving the differences $f(an+b)-f(cn+d)$, where a, b, c, d are fixed positive integers satisfying $ad-bc \neq 0$. This enabled him, for example, to show that an additive function, for which the limit $\lim_{n \to \infty} (f(an+b)-f(cn+d))$ exists, must satisfy $f(n)=\lambda \log n$ for some λ and all n coprime to $(ad-bc)ac$, thus solving a conjecture of Katai [11].

6. Multiplicative functions at consecutive integers

One may expect that the functions

$$f(n) = n^z \qquad (n \geq 1) \tag{8}$$

play an exceptional role among multiplicative functions similar to that of the functions (7) among additive functions, and one may try to find conditions on f, which imply (8). Recently, Wirsing (unpublished) proved that a multiplicative function f of modulus ≤ 1 and satisfying

$$\lim_{n\to\infty} \overline{f(n+1)}f(n) = 1 \tag{9}$$

must be of the form (8). This is the analogue of Erdös' result that for an additive function (5) implies (7). However, it has not yet been proved that the same conclusion holds, when (9) is replaced by the weaker condition

$$\lim_{x\to\infty} \frac{1}{x} \sum_{n\leq x} \overline{f(n+1)}f(n) = 1 \ ,$$

as was the case with Erdös' result. This is probably much more difficult than the corresponding result for additive functions.

On the whole, our present knowledge about the behavior of multiplicative functions at consecutive integers is very poor. It would be of great interest to determine the asymptotic behavior of the quantities

$$\frac{1}{x} \sum_{n\leq x} \overline{f(n+1)}f(n) \tag{10}$$

in the case $|f| \leq 1$, say, but almost nothing is known in this direction. In the case of the Moebius function, the obvious conjecture is that the limit of (10) is zero, but this seems to be unattackable at present and lies perhaps as deep as the twin prime conjecture. It is not even known whether $\mu(n+1)\mu(n)=-1$ holds on a set of positive density.

One can ask more generally for the simultaneous distribution of k consecutive values of f. Suppose, for example, that f is completely multiplicative and assumes only the values ± 1. For every k-tuple $\underline{\varepsilon} = (\varepsilon_1,\dots,\varepsilon_k)$, $\varepsilon_i = \pm 1$, let

$$N_{\underline{\varepsilon}}(x) = \#\{n \le x : f(n+i) = \varepsilon_i \ , \ i = 1,\dots,k\} \ .$$

Call f normal, if

$$N_{\underline{\varepsilon}}(x) \sim 2^{-k} x \qquad (x \to \infty)$$

holds for every $\underline{\varepsilon} = (\varepsilon_1,\dots,\varepsilon_k)$. Katai [13] has shown that, in a certain sense, almost all such functions f have this property. However, there is no specific function f, which has been proved to be normal. In particular, it is not known whether the Liouville-function $\lambda(n) = (-1)^{\Omega(n)}$ is normal, although this seems highly plausible.

While the last problem in its full generality seems to be unattackable at present, the case of two consecutive values is perhaps not completely out of reach. For example, it is easy to see that for $\underline{\varepsilon}=(1,1)$ and $\underline{\varepsilon}=(-1,-1)$ we have $N_{\underline{\varepsilon}}(x) \gg x$, $N_{\underline{\varepsilon}}(x)$ being defined as above with respect to the Liouville function. The cases $\underline{\varepsilon}=(1,-1)$ and $\underline{\varepsilon}=(-1,1)$ are much more difficult. Here one can show, by a relatively complicated argument, that $N_{\underline{\varepsilon}}(x) \gg x(\log\log x)^{-4}$ holds for arbitrary large values of x. There is still a great potential for further research, and the bound $N_{\underline{\varepsilon}}(x) \gg x$ for all choices of $\underline{\varepsilon}=(\varepsilon_1,\varepsilon_2)$ as a first major step towards the above mentioned general conjecture is perhaps not completely hopeless.

References

[1] H. Delange, Sur les fonctions arithmétiques multiplicatives. Ann. Sci. Ec. Norm. Sup. 78 (1961), 273-304.

[2] H. Delange, Théorie probabiliste des nombres. Astérisque 94 (1982), 31-42.

[3] P.D.T.A. Elliott, Probabilistic Number Theory I, II. Springer. New York 1979, 1980.

[4] P.D.T.A. Elliott, Arithmetic Functions and Integer Products. Springer. New York 1985.

[5] P. Erdös, On the distribution of additive functions. Ann. Math. 47 (1946), 1-20.

[6] P. Erdös and M. Kac, On the Gaussian law of errors in the theory of additive functions. Proc. Nat. Acad. Sci. U.S.A. 25 (1939), 206-207.

[7] G. Halász, Über Mittelwerte zahlentheoretischer Funktionen. Acta Math. Acad. Sci. Hung. 19 (1968), 365-403.

[8] G. H. Hardy and S. Ramanujan, The normal number of prime factors of a number n. Quart. J. Math. (Oxford) 48 (1917), 76-92.

[9] A. Hildebrand, On Wirsing's mean value theorem for multiplicative functions. Bull. London Math. Soc., to appear.

[10] A. Hildebrand, Multiplicative functions in short intervals. Preprint.

[11] I. Katai, Some results and problems in the theory of additive functions. Acta Sci. Math.(Szeged)30 (1969), 305-311.

[12] I. Katai, On a problem of P. Erdös. J. Number Theory 2 (1970),1-6.

[13] I. Katai, On random multiplicative functions. Acta Sci. Math. (Szeged) 33 (1972), 81-89.

[14] J. Kubilius, Probabilistic Methods in the Theory of Numbers. Am. Math. Soc. Transl. of Math. Monographs 11. Providence, 1964.

[15] J. Kubilius, Estimating the second central moment for arbitrary additive functions. Litovskii Mat. Sbornik 23 (1983) (2), 110-117.

[16] I. Z. Ruzsa, On the variance of an additive function. In: P. Erdös (Ed.), Studies in Pure Mathematics, to the memory of Paul Turán. Akademiai Kiado. Budapest 1983.

[17] H. N. Shapiro, Distribution functions of additive arithmetic functions. Proc. Nat. Acad. Sci. U.S.A. 42 (1956),426-430.

[18] P. Turán, On a theorem of Hardy and Ramanujan. J. London Math. Soc. 9 (1934), 274-276.

[19] E. Wirsing, Das asymptotische Verhalten von Summen über multiplikative Funktionen II. Acta Math. Sci. Hung. 18 (1967), 411-467.

[20] E. Wirsing, Characterization of the logarithm as an additive function. Am. Math. Soc. Proc. Symp. Pure Math. XX (1971), 375-381.

[21] E. Wirsing, Additive and completely additive functions with restricted growth. In: Recent Progress in Analytic Number Theory, Proc. of Symposium, Durham 1979. Vol. 2, 231-280. Academic Press, London 1981.

[22] E. Wirsing, Growth and differences of additive functions. Topics in Classical Number Theory. Colloquia Mathematica Societas Janos Bolyai 34, Budapest 1981, 1651-1661.

Adolf Hildebrand
Institute for Advanced Study
School of Mathematics
Princeton, New Jersey 08540
U. S. A.