An International Journal
computers & mathematics with applications

PERGAMON Computers and Mathematics with Applications 43 (2002) 1035–1061
www.elsevier.com/locate/camwa

Number Theory—Probabilistic, Heuristic, and Computational Approaches

K.-H. INDLEKOFER
Faculty of Mathematics and Informatics, University of Paderborn
Warburger Strasse 100, 33098 Paderborn, Germany
k-heinz@uni-paderborn.de

(Received and accepted March 2001)

Abstract—After the description of the models of Kubilius, Novoselov and Schwarz, and Spilker, respectively, a probability theory for finitely additive probability measures is developed by use of the Stone-Cech compactification of $\mathbb{N}$. The new model is applied to the result of Erdős and Wintner about the limit distribution of additive functions and to the famous result of Szemerédi in combinatorial number theory. Further, it is explained how conjectures on prime values of irreducible polynomials are used in the search for large prime twins and Sophie Germain primes. © 2002 Elsevier Science Ltd. All rights reserved.

Keywords—Probabilistic number theory, Asymptotic results on arithmetic function, Computational number theory, Stone-Cech compactification, Measure and integration on $\mathbb{N}$.

1. A SHORT HISTORICAL RETROSPECTIVE VIEW

Where are the roots of probabilistic number theory? Can they be found in the papers "Probabilité de certains faits arithmétiques" and "Eventualité de la division arithmétique" by Cesaro in 1884 and 1889, respectively, or in the assertions of Gauss in 1791 (see [1]), when he writes[1]
"Primzahlen unter $a(=\infty)$

$$\frac{a}{la}$$

Zahlen aus zwei Faktoren

$$\frac{lla \cdot a}{la}$$

wahrscheinlich aus 3 Faktoren

$$\frac{1}{2}\,\frac{(lla)^2 a}{la}$$

et sic in inf"?

If we say that probabilistic number theory is devoted to solving problems of arithmetic by using (ideas or) the machinery of probability, then the subject started not with Gauss, but *cum*

[1]In today's notation, let $\pi_k(x)$ denote the number of natural numbers not exceeding x which are made up of k distinct prime factors. Then, the above assertion can be understood as

$$\pi_k(x) \sim \frac{x}{\log x}\,\frac{(\log\log x)^{k-1}}{(k-1)!}, \qquad (x \to \infty).$$

PII: S0898-1221(01)00344-3

grano salis with the paper "The normal number of prime factors of a number n" by Hardy and Ramanujan [2]. They considered the arithmetical functions ω and Ω, where $\omega(n)$ and $\Omega(n)$ denote the number of different prime divisors and of all prime divisors—i.e., counted with multiplicity—of an integer n, respectively. Introducing the concept "normal order", Hardy and Ramanujan proved that ω and Ω have the normal order "$\log\log n$". Here we say, roughly, that an arithmetical function f has the normal order F, if $f(n)$ is approximately $F(n)$ for almost all values of n.[2] More precisely, this means that

$$(1-\varepsilon)F(n) < f(n) < (1+\varepsilon)F(n),$$

for every positive ε and almost all values of n.

In 1934, Turán [3] gave a new proof of Hardy and Ramanujan's result. It depended on the (readily obtained) estimate

$$\sum_{n\le x}(\omega(n)-\log\log x)^2 \le cx\log\log x.$$

This inequality—reminding us of Tschebycheff's inequality[3]—had a special effect, namely giving Kac the idea of thinking about the role of independence in the application of probability to number theory. Making essential use of the notation of independent random variables, the central limit theorem and sieve methods, Kac, together with Erdős, proved this in 1939 [5] and 1940 [6]. *For real-valued strongly additive functions f, let*

$$A(x) := \sum_{p\le x}\frac{f(p)}{p} \tag{1}$$

and

$$B(x) := \left(\sum_{p\le x}\frac{f^2(p)}{p}\right)^{1/2}. \tag{2}$$

Then, if $|f(p)|\le 1$ and if $B(x)\to\infty$ as $x\to\infty$, the frequencies

$$F_x(z) := \frac{1}{x}\#\left\{n\le x : \frac{f(n)-A(x)}{B(x)}\le z\right\}$$

converge weakly to the limit law

$$G(z) := \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{z} e^{-w^2/2}\,dw,$$

as $x\to\infty$ (which will be denoted by writing $F_x(z)\Rightarrow G(z)$).

Thus, for $f(n)=\omega(n)$, Erdős and Kac obtained a much more general result than Hardy and Ramanujan. For, in this case,

$$A(x) = \log\log x + O(1)$$

and

$$B(x) = (1+o(1))(\log\log x)^{1/2},$$

---

[2]A property E is said to hold for almost all n if $\lim_{x\to\infty} x^{-1}\#\{n\le x : E \text{ does not hold for } n\} = 0$.

[3]At that time, Turán knew no probability (see [4, Chapter 12]). The first widely accepted axiomatic system for the theory of probability, due to Kolmogorov, had only appeared in 1933.

so that

$$x^{-1}\#\left\{n \le x : \frac{\omega(n) - \log\log x}{\sqrt{\log\log x}} \le z\right\} \Rightarrow \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{z} e^{-w^2/2}\, dw.$$

A second effect of the above-mentioned paper of Turán was that Erdős, adopting Turán's method of proof, showed [7] that, whenever the three series

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

converge, then the real-valued strongly additive function f possesses a limiting distribution F, i.e.,

$$x^{-1}\#\{n \le x : f(n) \le z\} \Rightarrow F(z),$$

with some suitable distribution function F. It turned out [8] that the convergence of these three series was in fact necessary.

All these results can be described as effects of the fusion of (intrinsic) ideas of probability theory and asymptotic estimates. In this context, divisibility by a prime p is an event A_p, and all the $\{A_p\}$ are statistically independent of one another, where the underlying "measure" is given by the *asymptotic density*

$$\delta\left(A_p\right) := \lim_{x\to\infty} x^{-1}\#\left\{n \le x : n \in A_p\right\} = \lim_{x\to\infty} x^{-1} \sum_{\substack{n\le x \\ p|n}} 1 \left(= \frac{1}{p}\right). \tag{3}$$

(If the limit

$$M(f) := \lim_{x\to\infty} x^{-1} \sum_{n\le x} f(n)$$

exists, then we say that the function f possesses an (*arithmetical*) *mean-value* $M(f)$.) Then, for strongly additive functions f,

$$f = \sum_{p} f(p)\varepsilon_p,$$

where ε_p denotes the characteristic function of A_p and $M(\varepsilon_p) = 1/p$.

The main difficulties concerning the immediate application of probabilistic tools arise from the fact that the arithmetical mean-value (3) defines only a finitely additive measure (or content, or pseudo-measure) on the family of subsets of $\mathbb{N}$ having an asymptotic density. To overcome these difficulties, one builds a sequence of finite, purely probabilistic models, which approximate the number theoretical phenomena, and then use arithmetical arguments for "taking the limit". This theory, starting with the above-mentioned results of Erdős, Kac and Wintner, was developed by Kubilius [9]. He constructed finite probability spaces on which independent random variables could be defined so as to mimic the behaviour of truncated additive functions

$$\sum_{p\le r} f(p)\varepsilon_p.$$

This approach is effective if the ratio $\log r/\log x$ essentially tends to zero as x runs to infinity. Then, Kubilius was able to give necessary and sufficient conditions in order that the frequencies

$$x^{-1}\#\{n \le x : f(n) - A(x) \le zB(x)\}$$

converge weakly as $x \to \infty$, assuming that f belongs to a certain class of additive functions. This opened the door for the investigation of the *renormalization* of additive functions, i.e., determine when a given additive function f may be renormalized by functions $\alpha(x)$ and $\beta(x)$, so that as $x \to \infty$ the frequencies

$$x^{-1}\#\left\{n \le x : \frac{f(n) - \alpha(x)}{\beta(x)} \le z\right\}$$

possess a weak limit (see [4,9,10]).

All these methods have been developed for and adapted to the investigation of additive functions with their emphasis on sums of independent random variables. The investigation of (real-valued) multiplicative functions goes back to Bakstys [11], Galambos [12], Levin *et al.* [13], and uses Zolotarev's result [14] concerning the characteristic transforms of products of random variables.

We reformulate as follows. A *general problem of probabilistic number theory* is to find appropriate probability spaces where large classes of arithmetic functions can be considered as random variables.

Let us now turn to combinatorial number theory, where we concentrate on van der Waerden's theorem, and mention how, in this case, a probabilistic interpretation plays an essential role, too.

The well-known theorem of van der Waerden states (in one of several equivalent formulations) that, if $\mathbb{N}$ is partitioned into finitely many classes $\mathbb{N} = B_1 \cup B_2 \cup \cdots \cup B_h$, then at least one class contains finite arithmetic progression of arbitrary length. To prove van der Waerden's result, it clearly suffices to show that for each $l = 2, 3, \ldots$, some B_j contains an arithmetic progression of length $l + 1$; for some B_j will occur for infinitely many l and that will be the desired B_j.

Van der Waerden's theorem is one of a class of results in combinatorial number theory where a certain property is predicated of one of the sets of an arbitrary partition of $\mathbb{N}$ and these properties are translation invariant. And, in this case, one may conjecture that there is a measure of the size of a set that will guarantee the property. This was done in the 1930s by Erdős and Turán. More precisely, their conjecture asserts that a set of positive upper density possesses arithmetic progressions of arbitrary length. Roth [15], using analytic methods, showed in 1952 that a set of positive upper density contains arithmetic progressions of length 3. In 1969, Szemerédi [16] showed that such sets contain arithmetic progressions of length 4, and finally in 1975 [17], he proved the full conjecture of Erdős and Turán. More precisely, he showed the following.

Let $B \subset \mathbb{N}$ be such that for some sequence of intervals $[a_n, b_n]$ with $b_n - a_n \to \infty$, $\#(B \cap [a_n, b_n])/(b_n - a_n) \to \alpha > 0$, then B contains arbitrarily long arithmetic progressions.

Szemerédi used intricate combinatorial arguments for his proof. It turned out that the tool appropriate for handling Szemerédi's theorem is the theory of *measure preserving transformations*. Proving a multiple recurrence of Poincaré's recurrence theorem allowed the proof of Szemerédi's result and, in addition, a multidimensional analogue of Szemerédi's theorem (see [18,19]).

To end this introduction, we move to heuristic results about prime numbers. A statistical interpretation of the *prime number theorem*,

$$\pi(x) := \# \{p \le x : p \text{ prime}\} \sim \frac{x}{\log x}, \qquad \text{as } x \to \infty,$$

tells that the probability for a large number n being prime is $1/\log n$. If the events that a random integer n and the integer $n + 2$ are primes were statistically independent, then it would follow that the pair $(n, n + 2)$ are twin primes with probability $1/(\log n)^2$. Now, these events are not independent since, if n is odd, then $n + 2$ is odd, too, and so Hardy and Littlewood [20] conjectured that the correct probability should be

$$\frac{2C_2}{(\log n)^2},$$

where

$$C_2 = \prod_{p \ge 3} \left[1 - \frac{1}{(p-1)^2}\right]$$

is the so-called *twin prime constant*, which is approximately 0.6601618.... The type of their arguments can be applied to obtain similar conjectural asymptotic formulae for the number of prime-triplets or longer block of primes, and then agree very closely with the results of counts.

More general conjectures are due to Schinzel and Sierpinsky, and in 1962, Bateman *et al.* [21] indicated a quantitative form of these conjectures.

CONJECTURE. *Let $f_1, f_2, \dots, f_s$ be irreducible polynomials, with integer coefficients and positive leading coefficients. If $Q(N)$ denotes the number of integers $1 < n < N$ such that $f_1(n), \dots, f_s(n)$ are all primes, then*

$$Q(N) \sim C_{f_1 \dots f_s} \frac{1}{\deg(f_1) \dots \deg(f_s)} \sum_{2}^{N} \frac{1}{(\log(N))^s},$$

where

$$C_{f_1 \dots f_s} = \prod_p \left(1 - \frac{w(p)}{p}\right)\left(1 - \frac{1}{p}\right)^{-s},$$

here $w(p)$ denotes the number of solutions of the congruence

$$f_1(x) \dots f_s(x) \equiv 0 \ (\mathrm{mod}\, p).$$

As should be expected, the conjectures of Hardy and Littlewood, Schinzel and Sierpinsky, and Bateman and Horn inspired a considerable amount of computation, indeed to determine accurately the constants involved in the formulae, and to verify that the predictions fit well with the observations.

The aim of the first part of this paper is to describe a new theory which solves the above-mentioned general problem of probabilistic number theory and shows how, for example, Szemerédi's result fits into the framework of this theory.

In the second part, we focus on heuristic and computational results and sketch briefly how we could find the largest known twin primes.

2. APPROXIMATION OF INDEPENDENCE

In this section, we have in mind the idea of Kac that, suitably interpreted, divisibility of an integer by different primes represents independent events. At the beginning, we shall consider two examples of algebras of subsets of $\mathbb{N}$. We denote by $\mathcal{A}_1$ the algebra generated by all residue classes in $\mathbb{N}$, whereas $\mathcal{A}_2$ is defined as the algebra generated by the zero residue classes. On both algebras the asymptotic density is finitely but not countably additive. In the case of the algebra $\mathcal{A}_1$, this difficulty will be overcome by the embedding of $\mathbb{N}$ into the polyadic numbers. Concerning the algebra $\mathcal{A}_2$, a solution of the problem will be given by the construction of the model of Kubilius. In Section 5, we shall formulate a general solution of both of these problems.

For a natural number Q, let $E(l, Q)$ denote the set of positive integers n which satisfy the relation $n \equiv l \bmod Q$ where l assumes any value in the range $1 \le l \le Q$. Denote by $\mathcal{A}_1$ the algebra generated by all these arithmetic progressions $E(l, Q)$ for $Q = 1, 2, \dots,$ and $1 \le l \le Q$. Observe that each member $A \in \mathcal{A}_1$ possesses an asymptotic density $\delta(A)$ and δ is fully determined by the values

$$\delta(E(l, Q)) = \frac{1}{Q},$$

for each Q and all $1 \le l \le Q$. Then, δ is finitely additive but not countably additive on the algebra $\mathcal{A}_1$ which will be shown by an example due to Manin (see [22, p. 135]).

Let $Q_i = 3^i$, $i = 1, 2, \dots,$ and put $E_1 = E(0, Q_1)$ and $E_2 = (1, Q_2)$. For $j \ge 3$, choose l_j to be the smallest positive integer not occurring in $E_1 \cup E_2 \cup \dots \cup E_{j-1}$. Put $E_j = E(l_j, Q_j)$. It is clear that $\mathbb{N} = \bigcup_{i=1}^{\infty} E_i$. Further, $E_i \cap E_j = \emptyset$ if $i \ne j$. For this, suppose $j > i$ and $l_j + m_j Q_j = l_i + m_i Q_i$. We see that $l_j = l_i + Q_i(m_i - 3^{j-i} m_j)$ and, since $l_j > l_i$, $l_j \in E_i$, which contradicts the choice of l_j. Since

$$\sum_{i=1}^{\infty} \delta(E_i) = \sum_{i=1}^{\infty} 3^{-i} = \frac{1}{2} < 1 = \delta\left(\bigcup_{i=1}^{\infty} E_i\right),$$

the asymptotic density is not a measure on $\mathcal{A}_1$.

Concerning the definition of $\mathcal{A}_2$, we choose, for each prime p, the sets $A_{p^k} = E(0, p^k)$ of natural numbers which are divisible by p^k ($k = 1, 2, \dots$). Then, $\mathcal{A}_2$ will be the smallest algebra containing all the sets A_{p^k}. Obviously, $\mathcal{A}_2$ is a subalgebra of $\mathcal{A}_1$ and the asymptotic density δ is finitely additive. It is not difficult to show by an example that δ is not countably additive on $\mathcal{A}_2$.

In his book [9], Kubilius applies finite probabilistic models to approximate independence of the events A_p for primes p. The study of arithmetic functions within the classical theory of probability, with its emphasis on sums and products of independent random variables, involves a careful balance between the convenience of a measure, with respect to which appropriate events are independent, and the loss of generality for the class of functions which may be considered.

The models of Kubilius are constructed to mimic the behaviour of (truncated) additive functions by suitably defined independent random variables. The construction may run as follows (see [4, p. 119]).

Let $2 \le r \le x$, let $S := \{n : n \le x\}$, and put $D = \prod_{p \le r} p$. For each prime p dividing D, let $\tilde{E}(p) := S \cap E(0,p)$ and $\bar{E}(p) = S \setminus E(p)$. If we define, for each positive integer k which divides D, the set

$$E_k = \bigcap_{p|k} E(p) \bigcap_{p|(D/k)} \tilde{E}(p),$$

then these sets are disjoint for differing values of k. Further, if $\mathcal{A}$ denotes the σ-algebra which is generated by the $E(p)$, $p \le r$, then each member of $\mathcal{A}$ is a union of finitely many of the E_k. On the algebra $\mathcal{A}$, one defines a measure ν. If

$$A = \bigcup_{j=1}^{m} E_{k_j},$$

then

$$\nu(A) := \sum_{j=1}^{m} [x]^{-1} \left| E_{k_j} \right|.$$

Since $\nu(S) = 1$, the triple $(S, \mathcal{A}, \nu)$ forms a finite probability space. A second measure μ will be defined by

$$\mu(E_k) := \frac{1}{k} \prod_{p|(D/k)} \left(1 - \frac{1}{p}\right),$$

where $k \mid D$. It is clear that $\mu(S) = 1$, and thus, the triple $(S, \mathcal{A}, \mu)$ is also a finite probability space. By an application of the Selberg sieve method, one can show that

$$\nu(A) = \mu(A) + O(L),$$

holds uniformly for all sets A in the algebra $\mathcal{A}$ with

$$L = \exp\left(-\frac{1}{8} \frac{\log x}{\log r} \log\left(\frac{\log x}{\log r}\right)\right) + x^{-1/15}.$$

An immediate consequence of the above construction is as follows.

PROPOSITION 1. *(See [4, Lemma 3.2].) Let r and x be real numbers, $2 \le r \le x$. Define the strongly additive function*

$$g(n) = \sum_{\substack{p|n \\ p \le r}} f(p),$$

where the $f(p)$ assume real values. Define the independent random variables X_p on a probability space $(\Omega, \mathcal{A}, P)$, one for each prime not exceeding r, by

$$X_p = \begin{cases} f(p), & \text{with probability } \dfrac{1}{p}, \\ 0, & \text{with probability } 1 - \dfrac{1}{p}. \end{cases}$$

Then, the estimate

$$x^{-1}\#\{n \le x : g(n) \le z\} = P\left(\sum_{p\le r} X_p \le z\right) + O\left(\exp\left(-\frac{1}{8}\frac{\log x}{\log r}\log\left(\frac{\log x}{\log r}\right)\right)\right) + O\left(x^{1/15}\right)$$

holds uniformly for all real numbers $f(p), z, x (x \ge 2)$ *and* r $(2 \le r \le x)$.

The Kubilius model can be directly applied to obtain, in particular, the celebrated theorem of Erdős and Kac. For this, we confine our attention for the moment to (real-valued) strongly additive functions f and recall definitions (1) and (2) of $A(x)$ and $B(x)$. Following Kubilius, we shall say that f belongs to the class H if there exists a function $r = r(x)$ so that as $x \to \infty$,

$$\frac{\log r}{\log x} \to 0, \qquad \frac{B(r)}{B(x)} \to 1, \qquad B(x) \to \infty.$$

As an archetypal result, we mention the following (see [4, Theorem 12.1]).

PROPOSITION 2. *(See [9].) Let f be a strongly additive function of class H. Then, the frequencies*

$$x^{-1}\#\{n \le x : f(n) - A(x) \le zB(x)\} \tag{4}$$

converge to a limit with variance 1 as $x \to \infty$, if and only if there is a nondecreasing function K of unit variation such that at all points at which $K(u)$ is continuous,

$$\frac{1}{B^2(x)} \sum_{\substack{p\le x \\ f(p)\le uB(x)}} \frac{f^2(p)}{p} \to K(u),$$

as $x \to \infty$. When this condition is satisfied, the characteristic function ϕ of the limit law will be given by Kolmogorov's formula

$$\log \phi(t) = \int_{-\infty}^{\infty} \left(e^{itu} - 1 - itu\right) u^{-2}\, dK(u),$$

and the limit law will have mean zero, and variance 1. Whether frequencies (4) converge or not,

$$\begin{aligned} &\frac{1}{xB(x)} \sum_{n\le x} (f(n) - A(x)) \to 0, \\ &\frac{1}{xB^2(x)} \sum_{n\le x} (f(n) - A(x))^2 \to 1, \end{aligned} \tag{5}$$

holds as $x \to \infty$.

Bearing in mind that in the Kolmogorov representation of the characteristic function of the normal low with variance 1, we have

$$K(u) = \begin{cases} 1, & \text{if } u \ge 0, \\ 0, & \text{if } u < 0, \end{cases}$$

we arrive at the following (see [4, Theorem 12.3]).

PROPOSITION 3. *(See [5,6].) Let f be a real valued strongly additive function which satisfies $|f(p)| \le 1$ for every prime p. Let $B(x) \to \infty$ as $x \to \infty$. Then,*

$$x^{-1}\#\{n \le x : f(n) - A(x) \le zB(x)\} \Longrightarrow \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{z} e^{-w^2/2}\, dw.$$

REMARK. The value distribution of positive-valued arithmetic h may be studied in terms of

$$x^{-1}\#\{n \le x : \log h(n) - \alpha(x) \le z\beta(x)\},$$

with renormalizing constants $\alpha(x)$, $\beta(x) > 0$. For those functions which grow rapidly, there is another perspective. We say that the values of positive valued function h are uniformly distributed in $(0,\infty)$ if $h(n)$ tends to infinity as $n \to \infty$ and if there exists a positive constant c such that as $y \to \infty$,

$$N(h,y) := \sum_{\substack{n \\ h(n)\le y}} 1 = (c + o(1))y.$$

General results for multiplicative functions h in connection with the existence of the limiting distribution of h/id can be found in [23]. A detailed account concerning multiplicative functions is given by Diamond *et al.* [24].

3. FIRST MOTIVATION: UNIFORM INTEGRABILITY. APPLICATION

There are three results concerning the asymptotic behaviour of multiplicative functions $g : \mathbb{N} \to \mathbb{C}$ with $|g(n)| \le 1$ for all $n \in \mathbb{N}$ which have become classical.

(1) Delange [25] proved that the mean value $M(g)$ exists and is different from zero if and only if the series
$$\sum_p \frac{1-g(p)}{p} \tag{6}$$
converges, and for some positive r, $g(2^r) \ne -1$.

(2) Assuming that g is real-valued and series (6) diverges, Wirsing [26] proved that g has mean-value $M(g) = 0$. In particular, this means that the mean value $M(g)$ always exists for real-valued multiplicative functions of modulus ≤ 1.

(3) Halász [27] proved that the divergence of the series
$$\sum_p \frac{1 - \operatorname{Re} g(p)p^{-it}}{p},$$
for each $t \in \mathbb{R}$ implies that a complex-valued multiplicative g has mean value $M(g) = 0$. Furthermore, he gave a complete description of the means $M(g,x) := x^{-1}\sum_{n\le x} g(n)$ as $x \to \infty$.

REMARKS. If we set $g(n) = \mu(n)$, the Möbius function, then we are precisely concerned with the case where the series $\sum_p p^{-1}(1 - g(p))$ diverges. Moreover, the validity of the assertion $M(\mu) = 0$ was shown by Landau [28] to be equivalent to the prime number theorem. The (first) elementary proof of the prime number theorem by Selberg appeared in 1949. In 1943, Wintner [29], in his book on Erathostenian averages, asserted that if a multiplicative function g may have only values ± 1, then the mean value $M(g)$ always existed. But, the sketch of his proof could not be substantiated, and the problem remained open as the Erdős-Wintner conjecture. We shall not repeat the story concerning the prize which Erdős offered for a solution of this problem (cf. [4, p. 254]), but in 1967, Wirsing, by his result mentioned earlier, solved this problem. His proof was done by elementary methods (and thus, he gave another elementary proof of the prime number theorem), but he could not handle the complex-valued case in its full generality. Only by an analytic method, found by Halász in 1968, and exposed by him in his paper [27], the asymptotic behaviour of $\sum_{n\le x} g(n)$ could be fully determined for all complex-valued multiplicative functions g of modulus smaller than or equal to one. As in the case of Wirsing's proof of the Erdős-Wintner conjecture, it took another 24 years until Daboussi *et* *al.* [30] produced an elementary proof of Halász's theorem. In a subsequent paper, Indlekofer [31], following the same lines of the proof, gave a more elegant version which served as a model in the book of Schwarz *et al.* [32]. This ends the remarks.

The wish to abandon the restriction on the size of g led to the investigation of multiplicative functions which belong to the class $\mathcal{L}^q$, $q > 1$. Here, for $1 \le q \le \infty$,

$$\mathcal{L}^q := \{f : \mathbb{N} \to \mathbb{C}, \|f\|_q < \infty\}$$

denotes the linear space of arithmetic functions with bounded seminorm

$$\|f\|_q := \left\{ \limsup x^{-1} \sum_{n \le x} |f(n)|^q \right\}^{1/q}.$$

Obviously, the functions considered by Delange, Wirsing and Halász belong to every class $\mathcal{L}^q$.

A characterization of multiplicative functions $g \in \mathcal{L}^q$ ($q > 1$) which possess a nonzero mean-value $M(g)$ was independently given by Elliott [33] and using a different method, by Daboussi [34]. These results were the starting point for me to introduce the concept of *uniformly summable functions*.

The underlying motivations for this were the facts that

(i) if the mean-value $M(f)$ of an arithmetic function f corresponds to an integral over an (finite) integrable function, then it can be approximated by its truncation f_K at height K, i.e.,

$$f_K(n) = \begin{cases} f(n), & \text{if } |f(n)| \le K, \\ 0, & \text{if } |f(n)| > K, \end{cases}$$

(ii) and, on the other hand, the partial sums $\{N^{-1} \sum_{n \le N} f(n)\}_{N \in \mathbb{N}}$ converge to $M(f)$.

This suggested the involvement of the concept of *uniform integrability*. In 1980 [35], I introduced the following.

DEFINITION. *A function $f \in \mathcal{L}^1$ is said to be uniformly summable if*

$$\lim_{K \to \infty} \sup_{N \ge 1} N^{-1} \sum_{\substack{n \le N \\ |f(n)| > K}} |f(n)| = 0,$$

and the space of all uniformly summable functions is denoted by $\mathcal{L}^*$.

It is easy to show that, if $q > 1$,

$$\mathcal{L}^q \subset \mathcal{L}^* \subset \mathcal{L}^1.$$

Further, we note that $\mathcal{L}^*$ is nothing else but the $\| \cdot \|_1$-closure of l^∞, the space of all bounded functions on $\mathbb{N}$. In the same way, we can define the spaces

$$\mathcal{L}^{*q} := \| \cdot \|_q - \text{closure of } l^\infty.$$

The idea of uniform summability turned out to provide the appropriate tools for describing the mean behaviour of multiplicative functions and gave exact insight which additive functions belong to $\mathcal{L}^1$. As typical results, we mention generalizations of the results of Delange, Wirsing and Halász.

PROPOSITION 4. *(See [35].) (A generalization of Delange's result.) Let $g : \mathbb{N} \to \mathbb{C}$ be multiplicative and $q \ge 1$. Then, the following two assertions hold.*

(i) *If $g \in \mathcal{L}^* \cap \mathcal{L}^q$ and if the mean-value $M(g) := \lim_{x \to \infty} x^{-1} \sum_{n \le x} g(n)$ of g exists and is nonzero, then the series*

$$\sum_p \frac{g(p) - 1}{p}, \qquad \sum_{\substack{p \\ |g(p)| \le 3/2}} \frac{|g(p) - 1|^2}{p}, \qquad \sum_{\substack{p \\ |g(p) - 1| \ge 1/2}} \frac{|g(p)|^\lambda}{p}, \qquad \sum_p \sum_{k \ge 2} \frac{|g(p^k)|^\lambda}{p^k}, \tag{7}$$

converge for all λ *with* $1 \leq \lambda \leq q$, *and, for each prime* p,

$$1 + \sum_{k=1}^{\infty} \frac{g\left(p^k\right)}{p^k} \neq 0. \tag{8}$$

(ii) *If series (7) converge, then* $g \in \mathcal{L}^* \cap \mathcal{L}^q$ *and the mean-values* $M(g)$, $M(|g|^\lambda)$ *exist for all* λ *with* $1 \leq \lambda \leq q$. *If, in addition, (8) holds, then* $M(g) \neq 0$.

Note, that the membership of $\mathcal{L}^q \cap \mathcal{L}^*$ and the existence of a nonzero mean value are together equivalent to a set of explicit conditions on the prime powers. Further, observe that these conditions imply the existence of the mean values $M(|g|^\lambda)$ for all $1 \leq \lambda \leq q$.

PROPOSITION 5. *(See [23].) (A generalization of Wirsing's result.) Let* $g \in \mathcal{L}^*$ *be a real-valued multiplicative function. Then, the existence of the mean value* $M(|g|)$ *implies the existence of* $M(g)$.

Note that Proposition 5 is the appropriate generalization of Wirsing's result, for if g is multiplicative and $|g| \leq 1$, the mean value of $M(|g|)$ always exists.

In this connection, it is interesting to mention the following characterization of nonnegative multiplicative functions of $\mathcal{L}^*$ (see [36]).

Let $\varepsilon \geq 0$ *and* $g \in \mathcal{L}^{1+\varepsilon} \cap \mathcal{L}^*$ *be a nonnegative multiplicative function. If* $\|g\|_1 > 0$, *then* $g^{1+\varepsilon} \in \mathcal{L}^*$ *and there exist positive constants* c_1, c_2 *such that, as* $x \to \infty$,

$$M\left(g^{1+\varepsilon},\right) = \exp\left(\sum_{p\leq x} \frac{g^{1+\varepsilon}(p) - 1}{p}\right)(c_1 + o(1)) = \exp\left(\sum_{p\leq x} \frac{g(p) - 1}{p}\right)(c_2 + o(1)),$$

from which we deduce that the existence of $M(g^{1+\varepsilon})$ *implies the existence of* $M(g)$.

A complete characterization of the means $M(g, x)$ for complex-valued multiplicative functions $g \in \mathcal{L}^*$ was given in 1980 by Indlekofer (see [36]). As a special result, we have the following statement.

PROPOSITION 6. *(A generalization of Halász's result.) If the complex-valued multiplicative function* g *belongs to* $\mathcal{L}^*$, *and for each* $t \in \mathbb{R}$, *the series*

$$\sum_{\substack{p \\ ||g(p)|-1| \leq 1/2}} \frac{1 - \operatorname{Re} g(p)\left(|g(p)|\, p^{it}\right)^{-1}}{p}$$

diverges, then g *has mean value zero.*

Thus, the idea of uniformly summable functions proved to be a successful concept in the investigation of multiplicative functions (and, in particular, of additive functions, too). To come back to the methodological aspect and as an *a posteriori* justification of the underlying motivation, we turn to the connections between mean values and integrals for multiplicative and additive functions (see [23,37]).

PROPOSITION 7. *(See [23].) Let the real-valued multiplicative function* g *be uniformly summable. Then,*

(i) *g possesses a limiting distribution G if and only if the mean value* $M(|g|)$ *exists, and*
(ii) *this limiting distribution is degenerate if and only if* $M(|g|) = 0$.

Moreover, in both cases,

$$M(g) = \int_{\mathbb{R}} y \, dG(y), \qquad M(|g|) = \int_{\mathbb{R}} |y| \, dG(y).$$

PROPOSITION 8. *(See [37].) Let $q \geq 1$. For any (real-valued) additive function f, the following three propositions are equivalent.*

(i) *The limiting distribution F of f exists and*

$$\int_{\mathbb{R}} |y|^q \, dF(y) < \infty.$$

(ii) *$f \in \mathcal{L}^q$ and the mean value $M(f)$ of f exists.*

(iii) *The series*

$$\sum_p \frac{f(p)}{p}, \qquad \sum_{\substack{p \\ |f(p)| \leq 1}} \frac{f^2(p)}{p}, \qquad \sum_{\substack{p \\ |f(p^m)| \geq 1}} \sum_m \frac{|f(p^m)|^q}{p^m},$$

converge.

Moreover, if one of the above conditions is satisfied,

$$M(f) = \int_{\mathbb{R}} y \, dF(y), \qquad M(|f|^q) = \int_{\mathbb{R}} |y|^q \, dF(y).$$

REMARK. The "reason" for the difference between the additive and multiplicative functions may be found in the fact that there is no additive function in $\mathcal{L}^1 \setminus \mathcal{L}^*$, but there are "many" multiplicative functions in $\mathcal{L}^1$ which are not uniformly summable.

We do not want to obscure the leading thread of this section by a mass of details, but at the end, I would like to tell an anecdote about the encounter with a specific multiplicative function, *Ramanujan's τ function.*

In July 1983, my wife, my daughter, and I arrived in Urbana, Illinois for a visit of about three months. I was a guest at the Mathematical Department of the University of Illinois at Urbana-Champaign. In a series of lectures, I presented some of my results on multiplicative functions. As a specific example, I mentioned Ramanujan's function τ which is defined by the identity

$$\sum_{n=1}^{\infty} \tau(n) x^n = x \prod_{j=1}^{\infty} \left(1 - x^j\right)^{24}.$$

Putting $g(n) := \tau(n) \cdot n^{-11/2}$ leads to a real-valued multiplicative function g, satisfying the relations

$$g\left(p^{r+1}\right) = g(p) g\left(p^r\right) - g\left(p^{r-1}\right), \qquad r \geq 1,$$

and

$$|g(p)| \leq 2.$$

The first relation was established by Mordell [38] in 1917, whereas the second one was demonstrated by Deligne [39] in 1974 as a consequence of his proof of the Weil conjecture. In 1939, Rankin [40] obtained the asymptotic formula

$$\sum_{n \leq x} \tau(n)^2 = A x^{12} + O\left(x^{12-\delta}\right),$$

with some positive constants A, δ which implies that $g \in \mathcal{L}^2$, $M(g^2) \neq 0$, and $\sum_p p^{-1}(g^2(p) - 1)$ converges.

On Tuesday, July 26 of that year, I gave the second of the mentioned talks at the University of Illinois, Urbana-Champaign. By that time, matters had reached the stage that I could prove the following (cf. Proposition 5 and the following).

(i) Let $0 < \delta \leq 2$. Then, $M(|g|^\delta)$ exists. In particular, $M(g)$ exists.

(ii) If $M(|g|^{\delta}) \neq 0$ for some $0 < \delta < 2$ or if $g \in \mathcal{L}^q$ for some $q > 2$, then, for every positive β, $M(|g|^{\beta})$ exists and

$$\sum_p \frac{|g(p)|^{\beta} - 1}{p}$$

converges.

During the question period at the end of the lecture, a member of the audience, Carlos Moreno, informed me that he and Shahidi had proved that the function $\sum_{n=1}^{\infty} \tau(n)^4 n^{-22-s}$ had a double pole at $s = 1$ and that

$$\sum_p \frac{g(p)^4 - 2}{p}$$

converges. This yielded immediately the following result.

PROPOSITION 9. *Let $g(n) = \tau(n)n^{-11/2}$, where τ denotes Ramanujan's function. Then, the mean values $M(|g|^{\delta})$ are zero for $0 < \delta < 2$, $M(g^2) \neq 0$, and $g \notin \mathcal{L}^q$ for $q > 2$.*

There are further results (and conjectures) about finer behaviour of Ramanujan's τ function (see, for example, [41,42] for his encounters with Ramanujan's function $\tau(n)$).

I close this chapter with the conjecture of Lehmer [43] that $\tau(n) \neq 0$ for every n. This is equivalent to the nonvanishing of the Poincaré series P_n of weight 12 for every n. Serre [44] proved by an application of the Chebotarev density theorem that

$$\#\{p \leq x : \tau(p) = 0\} \ll \frac{x}{(\log x)^{1+\gamma}},$$

for some $\gamma > 0$. He further showed that, if the generalized Riemann hypothesis for Artin L-series is assumed, then

$$\#\{p \leq x : \tau(p) = 0\} \ll x^{3/4}.$$

Both estimates imply that those integers n for which $\tau(n) \neq 0$ have asymptotic density $\alpha > 0$. Lehmer's conjecture is equivalent to $\alpha = 1$ since τ is multiplicative.

4. POLYADIC NUMBERS: A FIRST ATTEMPT OF A GENERAL THEORY

The ring of polyadic numbers was first introduced by Prüfer [45]. We briefly recall its construction.

Let $\mathbb{Z}$ denote the ring of integers. Then, the system $\sum$ consisting of the ideals $(m) := m\mathbb{Z}$ can be taken as a complete system of neighborhoods of zero in the additive group of integers and it generates a topology which we denote by τ. Obviously, the addition is continuous in this topology and the arithmetic progressions $a + (m)$ $(a \in \mathbb{Z})$ build up a complete system of neighborhoods in $\mathbb{Z}$. The multiplication is continuous in the topology, too. For, if $a, b \in \mathbb{Z}$ and if W is any neighborhood of ab, for example, $W = ab + (m)$, then one can choose $U = a + (m)$ and $V = b + (m)$ as neighborhoods of a and b, respectively, such that $UV \subset W$. Therefore, $\mathbb{Z}$ endowed with the topology τ forms a topological ring $(\mathbb{Z}, \tau)$. The topological ring $(\mathbb{Z}, \tau)$ is metrizable. It is not difficult to show the result.

PROPOSITION 10. *The function $\varrho : \mathbb{Z} \times \mathbb{Z} \to [0,1]$,*

$$\varrho(x, y) = \sum_{m=1}^{\infty} \frac{1}{2^m} \left(\frac{x - y}{m} \right),$$

where (t) denotes the distance from t to the nearest integer, defines a metric on $\mathbb{Z}$ which metrizes $(\mathbb{Z}, \tau)$.

Next, we give a short review of how the polyadic numbers can be defined. Let S be the set of sequences $\{a_i\}$ of integers such that, given $\varepsilon > 0$, there exists an N such that $\varrho(a_i, a_j) < \varepsilon$ if both $i, j > N$. We call two such Cauchy sequences $\{a_i\}$ and $\{b_i\}$ equivalent if $\varrho(a_i, b_i) \to 0$ as $i \to \infty$. We define the set S of polyadic numbers to be the set of equivalence classes of Cauchy sequences.

One can define the sum (and the product) of two equivalence classes of Cauchy sequences by choosing a Cauchy sequence in each class, defining addition (and multiplication) term-by-term, and showing that the equivalence class of the sum (and the product) depends only on the equivalence class of the two summands (and of the two factors). This enables us to turn the set S of polyadic numbers into a ring. $\mathbb{Z}$ can be identified with a subring of S consisting of equivalence classes containing a constant Cauchy sequence. Finally, it is easy to prove that S is complete with respect to the (unique) metric which extends the metric ϱ on $\mathbb{Z}$. S is a compact space since $\mathbb{Z}$ is totally bounded. Thus, on the additive group of the ring S, as a compact group there exists a normalized Haar measure P defined on a σ-algebra $\mathcal{A}$ which contains the Borel sets in S such that $(S, \mathcal{A}, P)$ is a probability space. The measure of an arithmetic progression $\alpha + \beta D$ where $\alpha, \beta \in S$ and D is a natural number, is $1/D$. Therefore, embedding $\mathbb{Z}$ in S eliminates the difficulty associated with the fact that asymptotic density is not countably additive. This enabled Novoselov [46] to develop an "integration theory" for arithmetic functions f which can be approximated by periodic functions with integer period.

REMARK. The arithmetic in the ring S and certain aspects of polyadic analysis were investigated by Novoselov in a series of papers [46–50].

REMARKS. An arithmetic function f is called

$$\begin{aligned} &\tau\text{-periodic}, && \text{if } f(n+r) = f(n), \text{ for every } n \in \mathbb{N}, \\ &\tau\text{-even}, && \text{if } f(n) = f(\gcd(n,r)), \text{ for every } n \in \mathbb{N}. \end{aligned}$$

It can be shown that the vector space B_r of r-even functions can be generated by the Ramanujan-functions c_d defined by

$$c_d(n) := \sum_{t \mid \gcd(d,n)} t\mu\left(\frac{n}{t}\right),$$

where $d \mid r$, i.e.,

$$B_r = \mathrm{Lin}_{\mathbb{C}}[c_d : d \mid r],$$

whereas each element of the vector space D_r of r-periodic functions can be written as a linear combination of exponential functions, i.e.,

$$D_r := \mathrm{Lin}_{\mathbb{C}}[e_{a/r} : a = 1, 2, \ldots, r],$$

where $e_{a/r}$ is defined by

$$e_{a/r}(n) = \exp\left(2\pi i \frac{a}{r} n\right).$$

We put

$$B := \bigcup_{r=1}^{\infty} B_r \qquad \text{and} \qquad D := \bigcup_{r=1}^{\infty} D_r,$$

for the vector space of all even and all periodic functions, respectively. Finally, we define the vector space

$$A := \mathrm{Lin}_{\mathbb{C}}[e_\alpha : \alpha \in [0,1)].$$

Obviously,

$$B \subset D \subset A.$$

The $\|\cdot\|_q$ of B, D, and A leads to

- the space of *q-almost even functions*,
- the space of *q-limit-periodic functions*, and
- the space of *q-almost periodic functions*, respectively.

We note that Schwarz *et al.* [32,51] introduced a compactification $\mathbb{N}^*$ of $\mathbb{N}$ by

$$\mathbb{N}^* = \prod_{p \text{ prime}} \bar{N}_p,$$

where $\bar{N}_p$ denotes the one-point-compactification of the discrete topological spaces $N_p = \{1, p, p^2, \dots\}$. By this compactification, they could describe the "integration theory" of almost even functions.

The above-mentioned construction of the polyadic numbers was used for the investigation of limit-periodic functions, whereas Mauclaire [52] used the Bohr compactification of $\mathbb{Z}$ for the corresponding investigation of almost periodic functions. In [32], Schwarz *et al.* presented another construction of the compact space $\bar{\mathbb{N}}$ and the compact ring of polyadic numbers (or Prüfer ring) via Gelfand's theory of commutative Banach algebras.

Some comments are called for in connection with these examples. First of all, the special role played by the asymptotic (or logarithmic) density should be emphasized. Further, it is important to note that despite the *ad hoc* construction of the compactifications, the "size" of these spaces is very restricted; the Möbius μ function, for example, is not an element of any of these spaces.

To abandon all these restrictions, we shall make use of the Stone-Čech compactification of $\mathbb{N}$ which enables us to deal with arbitrary algebras of subsets of $\mathbb{N}$ together with arbitrary additive functions on these algebras.

5. SECOND MOTIVATION: PSEUDOMEASURES ON $\mathbb{N}$ AND THE STONE-CECH COMPACTIFICATION

Suppose that $\mathcal{A}$ is an *algebra of subsets of* $\mathbb{N}$, i.e.,

(i) $\mathbb{N} \in \mathcal{A}$,
(ii) $A, B \in \mathcal{A} \Rightarrow A \cup B \in \mathcal{A}$,
(iii) $A, B \in \mathcal{A} \Rightarrow A \setminus B \in \mathcal{A}$.

Then, if $\mathcal{E}$ denotes the family of simple functions on $\mathbb{N}$, the set

$$\mathcal{E}(\mathcal{A}) := \left\{ s \in \mathcal{E}, s = \sum_{j=1}^{m} \alpha_j 1_{A_j}; \alpha_j \in \mathbb{C}, A_j \in \mathcal{A}, j = 1, \dots, m \right\}$$

of *simple functions on* $\mathcal{A}$ is a vector space. In [53], I investigated the $\|\cdot\|_q$-closure of $\mathcal{E}(\mathcal{A})$, the space of $\mathcal{L}^{*q}(\mathcal{A})$-*uniformly summable functions for the algebras* $\mathcal{A}$ whose elements possess an asymptotic density.

These results performed the initial steps towards the idea which can be described as follows: $\mathbb{N}$, endowed with the discrete topology, will be embedded in a compact space $\beta\mathbb{N}$, the Stone-Cech compactification of $\mathbb{N}$, and then any algebra $\mathcal{A}$ in $\mathbb{N}$ with an arbitrary finitely additive set function, a content or pseudomeasure on $\mathbb{N}$, can be extended to an algebra $\bar{\mathcal{A}}$ in $\beta\mathbb{N}$ together with an extension of this pseudomeasure, which turns out to be a premeasure on $\bar{\mathcal{A}}$. The basic necessary concepts are summarized in the following three propositions.

PROPOSITION 11. *There exists a compactification $\beta\mathbb{N}$ of $\mathbb{N}$ with the following equivalent properties.*

(i) *Every mapping f from $\mathbb{N}$ into any compact space Y has a continuous extension $\bar{f}$ from $\beta\mathbb{N}$ into Y.*

(ii) *Every bounded function on* $\mathbb{N}$ *has an extension to a function in* $C(\beta\mathbb{N})$.

(iii) *For any two subsets* A *and* B *of* $\mathbb{N}$,

$$\overline{A \cap B} = \bar{A} \cap \bar{B},$$

where $\bar{A} = \mathrm{cl}_{\beta\mathbb{N}} A$ *and* $\bar{B} = \mathrm{cl}_{\beta\mathbb{N}} B$ *are the closures of* A *and* B *in* $\beta\mathbb{N}$, *respectively.*

(iv) *Any two disjoint subsets of* $\mathbb{N}$ *have disjoint closures in* $\beta\mathbb{N}$.

Stone and Cech (see, for example, [54]) have investigated the compactification βX for completely regular spaces X. The above proposition contains their results for $X = \mathbb{N}$. An immediate consequence of (iii) is the following statement.

PROPOSITION 12. *The compactification* $\beta\mathbb{N}$ *of* $\mathbb{N}$ *has the following property.*

(v) *For any algebra* $\mathcal{A}$ *in* $\mathbb{N}$, *the family*

$$\bar{\mathcal{A}} := \{\bar{A} : A \in \mathcal{A}\}$$

is an algebra in $\beta\mathbb{N}$. *This property is equivalent to Properties (i)–(iv) of Proposition 11.*

It should be observed that $\beta\mathbb{N}$ is unique in the following sense: if a compactification $\tilde{\mathbb{N}}$ of $\mathbb{N}$ satisfies any one of the listed conditions, then there exists a homeomorphism of $\beta\mathbb{N}$ onto $\tilde{\mathbb{N}}$ that leaves $\mathbb{N}$ pointwise fixed.

As a consequence of Property (i), we obtain the following.

The identity mapping $\iota : \mathbb{N} \to \beta\mathbb{N}$ is a continuous monomorphism, which sends $\mathbb{N}$ onto a dense subset of $\beta\mathbb{N}$, such that the adjoint homomorphism

$$\iota^* : C(\beta\mathbb{N}) \to C^b(\mathbb{N}), \qquad \iota^*\left(\bar{f}\right) = \bar{f} \circ \iota,$$

maps $C(\beta\mathbb{N})$ isomorphically and isometrically (relative to the uniform metric) onto $C^b(\mathbb{N})$.

We are now in position to formulate the following fundamental result.

PROPOSITION 13. *Let* $\mathcal{A}$ *be an algebra in* $\mathbb{N}$ *and* $\delta : \mathcal{A} \to [0, \infty)$ *be a content on* $\mathcal{A}$, *(i.e., a finitely additive measure). Then, the map*

$$\bar{\delta} : \bar{\mathcal{A}} \to [0, \infty), \qquad \bar{\delta}\left(\bar{A}\right) = \delta(A),$$

is σ*-additive on* $\bar{\mathcal{A}}$ *and can uniquely be extended to a measure on the minimal* σ*-algebra* $\sigma(\bar{\mathcal{A}})$ *over* $\bar{\mathcal{A}}$.

PROOF. Obviously, $\bar{\delta}$ is a content on $\bar{\mathcal{A}}$. Therefore, we have to show only that $\bar{\delta}$ is continuous from above at the empty set $\emptyset$. Suppose $\{\bar{A}_n\}, \bar{A}_n \in \bar{\mathcal{A}}$, is a monotone decreasing sequence converging to $\emptyset$. Then, by the compactness of $\beta\mathbb{N}$, there exists $n_0 \in \mathbb{N}$ such that $\bar{A}_n = \emptyset$ for all $n \geq n_0$, and thus, Proposition 13 holds. ∎

The extension of $\bar{\delta}$ is also denoted by $\bar{\delta}$. We remark, as an immediate implication of the above construction, the following.

THEOREM.

(i) *Every finitely additive function on an algebra* $\mathcal{A}$ *in* $\mathbb{N}$ *can be extended to a finitely additive function on the algebra of all subsets of* $\mathbb{N}$.

(ii) *Every linear functional on the vector space* $\mathcal{E}(\mathcal{A})$ *can be extended to a linear functional on* $l^\infty (= C^b(\mathbb{N}))$.

In the second part of this section, we shall concentrate on the following topics:

- candidates for measures,
- spaces of arithmetic functions,
- integration theory for uniformly $\mathcal{A}_\delta$-summable functions,
- measure preserving systems.

We should have in mind that these results can be generalized in many directions.

Especially, we observe that the same integration theory can be done for any (infinite) set X (endowed with the discrete topology) and any pseudomeasure on X.

5.1. Candidates for Measures

Let $\Gamma = (\gamma_{nk})$ be a Toeplitz matrix, i.e., an infinite matrix $\Gamma = (\gamma_{nk})_{n,k\in\mathbb{N}}$ with nonnegative real elements γ_{nk} satisfying the following conditions:

(i) $\sup_n \sum_{k=1}^{\infty} \gamma_{nk} < \infty$,
(ii) $\gamma_{nk} \to 0$, $(n \to \infty$, k fixed),
(iii) $\sum_{k=1}^{\infty} \gamma_{nk} \to 1$, $(n \to \infty)$.

For a given Toeplitz matrix Γ, we define $\delta_\Gamma(A)$ for $A \subset \mathbb{N}$ by

$$\delta(A) := \delta_\Gamma(A) := \lim_{n\to\infty} \sum_{k=1}^{\infty} \gamma_{nk} 1_A(k),$$

if the limit exists. Then, if $\mathcal{A}_\delta$ is an algebra in $\mathbb{N}$ such that $\delta(A)$ exists for all $A \in \mathcal{A}_\delta$, the above construction leads to the probability space $(\beta\mathbb{N}, \sigma(\bar{\mathcal{A}}_\delta), \bar{\delta})$. We observe that

$$\|f\| := \|f\|_\Gamma := \limsup_{n\to\infty} \sum_{k=1}^{\infty} \gamma_{nk} |f(k)|$$

defines a *seminorm* on the space of functions f for which $\|f\| < \infty$.

REMARK. Toeplitz showed that (i)–(iii) characterize all those infinite matrices which map the linear space of convergent sequences into itself, leaving the limits of each convergent sequence invariant.

EXAMPLES.

(i) Choosing

$$\gamma_{nk} = \begin{cases} \dfrac{1}{n}, & \text{if } k \le n, \\ 0, & \text{if } k > n, \end{cases}$$

defines Cesaro's summability method and leads to *asymptotic density* and to the seminorm

$$\|f\| := \limsup_{n\to\infty} n^{-1} \sum_{k\le n} |f(k)|.$$

(ii) If we put

$$\gamma_{nk} := \begin{cases} \dfrac{1}{\log n} \dfrac{1}{k}, & \text{if } k \le n, \\ 0, & \text{if } k > n, \end{cases}$$

we obtain *logarithmic density* with the seminorm

$$\|f\| = \limsup_{n\to\infty} \frac{1}{\log n} \sum_{k\le n} \frac{|f(k)|}{k}.$$

(iii) Let $\{I_n\}$ be a sequence of nonempty intervals in $\mathbb{N}$, $I_n = [a_n, b_n]$ such that $b_n - a_n \to \infty$, if $n \to \infty$. We define

$$\gamma_{nk} = \begin{cases} \dfrac{1}{b_n - a_n}, & \text{if } k \in I_n, \\ 0, & \text{otherwise}. \end{cases}$$

If $A \subset \mathbb{N}$ is given and, for some sequences $\{I_n\}$ of such intervals, the limit

$$\delta(A) := \lim_{n\to\infty} \frac{|(A \cap I_n)|}{b_n - a_n}$$

exists, we say that A possesses a *Banach-density*.

(iv) Let $g : \mathbb{N} \to \mathbb{R}^+$ be a nonnegative function with $g(1) > 0$. We put

$$\gamma_{nk} = \begin{cases} \left(\sum_{m \le n} g(m) \right)^{-1} g(k), & \text{if } k \le n, \\ 0, & \text{if } k > n, \end{cases}$$

and assume that $\gamma_{nk} \to 0$ as $n \to \infty$ (k fixed). If the limit

$$M_g(f) := \lim_{n \to \infty} \left(\sum_{m \le n} g(m) \right)^{-1} \sum_{k \le n} f(k) g(k)$$

exists, we say that f possesses a mean-value with weight g and denote this mean by $M_g(f)$.

5.2. Spaces of Arithmetic Functions

Let δ be a set function defined by some Toeplitz matrix Γ and let $\mathcal{A} = \mathcal{A}_\delta$ be an algebra in $\mathbb{N}$ such that $\delta(A)$ is defined for all $A \in \mathcal{A}$, i.e., if $\Gamma = (\gamma_{nk})$,

$$\delta(A) := \lim_{n \to \infty} \sum_{k=1}^{\infty} \gamma_{nk} 1_A(k)$$

exists for every $A \in \mathcal{A}$. Further, let $\| \cdot \| = \| \cdot \|_\Gamma$ be the corresponding seminorm. Then, we introduce the following spaces.

DEFINITION 1. *Denote by $\mathcal{L}^{*1}(\mathcal{A})$ the $\| \cdot \|$-closure of $\mathcal{E}(\mathcal{A})$. A function $f \in \mathcal{L}^{*1}(\mathcal{A})$ is called uniformly $(\mathcal{A})$-summable. By $L^{*1}(\mathcal{A})$, we denote the quotient space $\mathcal{L}^{*1}(\mathcal{A})$ modulo null-functions (i.e., functions f with $\|f\| = 0$).*

DEFINITION 2.

(i) *A nonnegative arithmetic function f is called $\mathcal{A}$-measurable in case each truncation $f_K = \min(K, f)$ lies in $\mathcal{L}^{*1}(\mathcal{A})$ and f is tight, i.e., for every $\varepsilon > 0$, the estimate*

$$\limsup_{n \to \infty} \sum_{\substack{k=1 \\ |f(k)| > K}}^{\infty} \gamma_{nk} < \varepsilon$$

holds for some K.

(ii) *A real-valued arithmetic function is called $\mathcal{A}$-measurable in case its positive and negative parts f^+ and f^- are $\mathcal{A}$-measurable.*

(iii) *A complex-valued arithmetic function f is called $\mathcal{A}$-measurable in case* $\operatorname{Re} f, \operatorname{Im} f$ *are $\mathcal{A}$-measurable. The space of all $\mathcal{A}$-measurable functions is denoted by $\mathcal{L}^*(\mathcal{A})$. Further, we define $L^*(\mathcal{A})$ as $\mathcal{L}^*(\mathcal{A})$ modulo null-functions, i.e., functions f for which $\delta(\{m : f(m) \neq 0\}) = 0$.*

5.3. Integration Theory for Uniformly $\mathcal{A}$-Summable Functions

A first consequence of Proposition 13 is that, for all $s \in \mathcal{E}(\mathcal{A})$,

$$\lim_{n \to \infty} \sum_{k=1}^{\infty} \gamma_{nk} s(k) = \int_{\beta\mathbb{N}} \bar{s} \, d\bar{\delta},$$

where $\bar{s} : \beta\mathbb{N} \to \mathbb{C}$ denotes the extension of s.

Starting from this, we consider measurable and integrable functions on the probability space $(\beta\mathbb{N}, \sigma(\bar{\mathcal{A}}), \bar{\delta})$ and relate these to the functions from $\mathcal{L}^*(\mathcal{A})$.

The probability space $(\beta\mathbb{N}, \sigma(\bar{\mathcal{A}}), \bar{\delta})$ leads to the well-known space

$$L(\bar{\delta}) := L(\beta\mathbb{N}, \sigma(\bar{\mathcal{A}}), \bar{\delta}) = \{\bar{f} : \beta\mathbb{N} \to \mathbb{C}, \sigma(\bar{\mathcal{A}})\text{-measurable}\},$$

modulo null-functions, and

$$L^1(\bar{\delta}) := L^1(\beta\mathbb{N}, \sigma(\bar{\mathcal{A}}), \bar{\delta}) = \{\bar{f} : \beta\mathbb{N} \to \mathbb{C}, \|\bar{f}\| < \infty\},$$

modulo null-functions, with norm

$$\|\bar{f}\| := \int_{\beta\mathbb{N}} |\bar{f}| \, d\bar{\delta}.$$

A connection between the spaces $\mathcal{L}^*(\mathcal{A})$ and $\mathcal{L}^{*1}(\mathcal{A})$ and the spaces L and L^1, respectively, is given by the following statement.

PROPOSITION 14.

(i) *There exists a vector-space isomorphism*

$$^- : L^*(\mathcal{A}) \to L(\bar{\delta}),$$

such that

$$\bar{s} = \iota^{*-1}(s), \qquad \textit{for every } s \in \mathcal{E}(\mathcal{A}).$$

(ii) *There exists a norm-preserving vector-space isomorphism*

$$^- : L^{*1}(\mathcal{A}) \to L^1(\bar{\delta}),$$

such that

$$\bar{s} = \iota^{*-1}(s), \qquad \textit{for every } s \in \mathcal{E}(\mathcal{A}).$$

PROOF. (i) By Definition 2, we may restrict to nonnegative functions. Assume that $f \in \mathcal{L}^*(\mathcal{A})$ is nonnegative, and let $\{s_n\}$ be a sequence of nonnegative simple functions from $E(\mathcal{A})$ which define f (see Definition 2). Then, $\bar{s}_n$ converges on $\beta\mathbb{N}$ to a $\bar{\delta}$-measurable function $\bar{f}$, which is finite $\bar{\delta}$-almost everywhere.

Therefore, by reducing modulo null-functions, one obtains a well-defined 1-1 linear map $^-$: $L^*(\mathcal{A}) \to L(\bar{\delta})$ whose restriction to $\mathcal{E}(\mathcal{A})$ is given by ι^{*-1}. The map $^-$ preserves the distribution function, which means that the (limit) distribution of $f \in L^*(\mathcal{A})$ coincides with the distribution of $\bar{f} \in L(\bar{\delta})$. Finally, in order to show that $^-$ is onto, we choose for a given nonnegative $\bar{f} \in L(\bar{\delta})$ a sequence $\{\bar{s}_n\}$ of simple functions from $\mathcal{E}(\bar{\mathcal{A}})$ such that $\bar{s}_n$ converges to $\bar{f}$ $\bar{\delta}$-everywhere. (This choice is possible because $\sigma(\bar{\mathcal{A}})$ is generated by $\bar{\mathcal{A}}$.) The restrictions s_n to $\mathbb{N}$ converge to some $f \in \mathcal{L}^*(\mathcal{A})$ and (i) is proved for nonnegative functions. The general case then follows immediately. The proof of (ii) runs on the same lines as above. The map $^-$ is constructed in the following way. Given $f \in L^*(\mathcal{A})$, choose a sequence $\{s_n\}$ of simple functions from $\mathcal{E}(\mathcal{A})$ such that $\|f - s_n\| \to 0$ as $n \to \infty$. Then, the functions $\bar{s}_n = \iota^{*-1}(s_n)$ form a Cauchy sequence in L^1 and the limit $\bar{f}$ is the desired image of f in L^1. These remarks complete the proof of Proposition 14. ∎

REMARK. Choosing the algebras $\mathcal{A}_1$ and $\mathcal{A}_2$ of Section 2, together with the asymptotic density δ, leads to the same spaces of arithmetic functions which are considered in the mentioned "integration theory" by Novoselov and Schwarz and Spilker, respectively.

5.4. Measure Preserving Systems

Let

$$S : \mathbb{N} \to \mathbb{N}, \qquad S(n) = n + 1,$$

be the *shift operator* on $\mathbb{N}$, and let $\bar{S}$ be its unique extension to $\beta\mathbb{N}$. If δ is finitely additive on an algebra $\mathcal{A}$ and if $\delta(SA) = \delta(A)$ for every $A \in \mathcal{A}$, then the extension according to Proposition 14 leads to the measure preserving system

$$\left(\beta\mathbb{N}, \sigma\left(\bar{\mathcal{A}}\right), \bar{\delta}, \bar{S}\right). \tag{9}$$

For this, we obtain the following by the mentioned result of Fürstenberg.

PROPOSITION 15. *(See [18,55].) Let $\bar{\delta}(\bar{B}) > 0$. Then, for any $k > 1$, there exists $n \neq 0$ with*

$$\bar{\delta}\left(\bar{B} \cap \bar{S}^n \bar{B} \cap \cdots \cap \bar{S}^{(k-1)n} \bar{B}\right) > 0.$$

This implies the following result.

PROPOSITION 16. *Let the measure preserving system (9) be given. If B is a subset of $\mathbb{N}$ with $\delta(B) > 0$, then B contains arbitrary long arithmetic progressions.*

Let B be a subset of $\mathbb{N}$ with positive *upper Banach density*, i.e.,

$$\limsup_{|I| \to \infty} \frac{|B \cap I|}{|I|} > 0,$$

where I ranges over intervals of $\mathbb{N}$. Consider the algebra $\mathcal{A}$, which is generated by the translations

$$\{S^n B : n = 0, 1, 2, \dots, \}.$$

The algebra $\mathcal{A}$ is countable, and thus, there exists a sequence of intervals $\{I_n\}$, $I_n = [a_n, b_n]$, $b_n - a_n \to \infty$ such that

$$\delta(A) := \lim_{n \to \infty} \frac{|A \cap I_n|}{b_n - a_n}$$

exists for all $A \in \mathcal{A}$. Then, Proposition 16 gives the earlier mentioned result of Szemerédi [17].

6. ADDITIONAL REMARKS

The algebra $\mathcal{A}_2$, introduced in Section 2, can be defined as the algebra in $\mathbb{N}$ which is generated by the sets

$$A_{p^k} := \{n : p^k \| n\}$$

(p prime, $k = 1, 2, \dots$), whereas the algebra $\mathcal{A}_1$ (loc. cit.) is generated by the sets

$$A\left(l, p^k\right) = l + A_{p^k}, \qquad (p \text{ prime}, \ k = 1, 2, \dots),$$

with $l = 1, \dots, p^k$. In both cases, one can choose the asymptotic density δ as a suitable pseudomeasure. We concentrate on $(\mathcal{A}_2, \delta)$ and observe that, if the real-valued additive function f is given, we can put

$$f = \sum_p f_p,$$

where f_p is defined by

$$f_p(n) = \begin{cases} f\left(p^k\right), & \text{if } p^k \| n, \\ 0, & \text{otherwise.} \end{cases}$$

Obviously, every f_p is uniformly $\mathcal{A}$-summable, and we denote by $\bar{f}_p$ its unique extension to an integrable function on $\beta\mathbb{N}$. Then, $\{\bar{f}\}_{p \text{ prime}}$ is a set of independent random variables and $\sum_p \bar{f}_p$ converges, a.s., if and only if f possesses a limit distribution. This result can be seen as another *a posteriori* justification of the already mentioned idea of Kac concerning the role of independence in probabilistic number theory.

Concerning the *renormalization of additive functions* (see Proposition 2), we consider the increasing sequence $\sigma(\bar{\mathcal{A}}_n)$ of σ-algebras where $\bar{\mathcal{A}}_n$ is generated by

$$\{\bar{A}_{p^k} : p \leq n, k \in \mathbb{N}\}.$$

Obviously,

$$\bigcup_{n\in\mathbb{N}} \sigma\left(\bar{\mathcal{A}}_n\right) = \sigma\left(\bar{\mathcal{A}}_2\right).$$

Centering the independent random variables $\{\bar{f}_p\}$ at expectations leads to the martingale $\{\bar{S}_n\}_{n=1,2,\dots}$, where

$$\bar{S}_n = \sum_{i=1}^{n} \left(\bar{f}_{p_i} - \mathbb{E}\left(\bar{f}_{p_i}\right)\right).$$

Using the Lindeberg-Levy theorem for martingales, one can prove Proposition 2. In the case of multiplicative functions, we proceed in a similar manner. If a real-valued multiplicative function g is given, we put

$$g = \prod_p g_p,$$

where

$$g_p(n) = \begin{cases} g\left(p^k\right), & \text{if } p^k \| n, \\ 1, & \text{otherwise.} \end{cases}$$

The unique extension $\bar{g}_p$ of g_p builds a set $\{\bar{g}_p\}$ of independent random variables, and an application of Zolotarev's result gives necessary and sufficient conditions for the convergence of the product $\prod_p \bar{g}_p$ which turns out to be equivalent to the existence of the limit distribution of g.

The compactification of $\mathbb{N}$ which are given by $\mathbb{N}^*$ and which are induced by the constructions of the polyadic numbers and by the Bohr compactification of $\mathbb{Z}$, respectively, can be identified with compact subspaces of $\beta\mathbb{N}$.

7. PRIMES PLAY A GAME OF CHANCE

This is the headline of Chapter 4 in Kac's book [56], where he describes the statistics of Euler's φ-function and the function ω. Keeping this picturesque language, one can say that the primes grow like weeds among the natural numbers, seeming to obey no other law than that of chance, and nobody can predict where the next one will sprout. On the other hand, there are laws governing their behaviour, and they obey these laws with almost military precision.

One such law is intimately connected with the behaviour of $\pi(x)$, the number of primes not exceeding x (see the above-mentioned prime number theorem and its statistical interpretation). *Euclid's second theorem* states that the number of primes is infinite, i.e., $\pi(x)$ tends to infinity as $x \to \infty$. Here, we offer an elementary "probabilistic" proof of this assertion. For this, we choose the algebra $\mathcal{A}_3$ generated by $\{A_{p_i}\}_{i=1}^{\infty}$ where A_{p_i} consists of all multiples of p_i and the p_is run through the set of all primes. This leads to the probability space $(\beta\mathbb{N}, \sigma(\bar{\mathcal{A}}_3), \bar{\delta})$ where $\bar{\delta}$ is the extension of the asymptotic density δ. If $\bar{A} \in \sigma(\bar{\mathcal{A}}_3)$ and $\bar{\delta}(\bar{A}) > 0$, then $\bar{A}$ obviously contains infinitely many natural numbers.

Consider now the set $A = \bigcup_{i=1}^{\infty} A_{p_i}$. Since the family $\{\bar{A}_{p_i}\}_{i=1}^{\infty}$ of events is independent, we conclude that for any finite set $\mathcal{J} \subset \{1, 2, \dots\}$,

$$\beta\mathbb{N} \setminus \bigcup_{i\in\mathcal{J}} \bar{A}_{p_i} = \bigcap_{i\in\mathcal{J}} \left(\beta\mathbb{N} \setminus \bar{A}_{p_i}\right)$$

and

$$\bar{\delta}\left(\bigcap_{i\in\mathcal{J}}(\beta\mathbb{N}\setminus\bar{A}_{p_i})\right)=\prod_{i\in\mathcal{J}}\left(1-\frac{1}{p_i}\right)>0.$$

The only natural number not belonging to A is 1. Hence, A is clearly not a finite union of the A_{p_i}s, which proves that there is an infinity of primes.

Let us now turn to the theme of the predictability of the prime numbers. As already mentioned, the probability for a number of the order of magnitude x to be prime roughly equals $1/\log x$. An easy heuristic argument caused Hardy and Littlewood [20] to conjecture $2C_2/(\log x)^2$ as the expected probability for a twin prime $(n, n+2)$ when n is of the order of magnitude x. That is, the number of primes and twin primes in an interval of length a about x should be approximately $a/\log x$ and $2aC_2/(\log x)^2$, respectively, at least if the interval is long enough to make statistics meaningful, but small in comparison to x.

Table 1.

Interval	Primes		Twin Primes	
	Expected	Found	Expected	Found
$[10^8,\ 10^8+150000]$	8142	8145	584	601
$[10^9,\ 10^9+150000]$	7238	7242	461	466
$[10^{10}, 10^{10}+150000]$	6514	6511	374	389
$[10^{11}, 10^{11}+150000]$	5922	5974	309	276
$[10^{12}, 10^{12}+150000]$	5429	5433	259	276
$[10^{13}, 10^{13}+150000]$	5011	5065	221	208
$[10^{14}, 10^{14}+150000]$	4653	4643	191	186
$[10^{15}, 10^{15}+150000]$	4343	4251	166	161

The data of Table 1 are due to Jones *et al.* [57].

As one can see, the agreement with the theory is extremely good. This is especially surprising in the case of the twin primes, since it is not known whether there is an infinity of such pairs.

8. COMPUTATIONAL RESULTS (TOGETHER WITH JÁRAI)

As a last illustration of the predictability of primes, we turn to the above-mentioned conjecture of Bateman and Horn. The simple idea of this conjecture is again that the probability of a large number n being prime is $1/\log n$. Thus, the probability that the large numbers $f_1(n),\dots,f_s(n)$ are simultaneously prime is, if these events are independent,

$$\frac{1}{\log f_1(n)\dots\log f_s(n)}.$$

However, the s-tuples $(f_1(n),\dots,f_s(n))$ are not random. The constant $C_{f_1\dots f_s}$ should be viewed as measuring the extent to which the above events are not independent. Hence, it is reasonable to state the probability that $f_1(n),\dots,f_s(n)$ are simultaneously prime is

$$\frac{C_{f_1\dots f_s}}{\log f_1(n)\dots\log f_s(n)}.$$

Hence, the expected number $Q(a,b)$ of ns in $[a,b)$ for which $f_1(n),\dots,f_s(n)$ are simultaneously prime is

$$Q(a,b)\sim C_{f_1\dots f_s}\int_a^b\frac{du}{\log f_1(u)\dots\log f_s(u)}. \tag{10}$$

We used this heuristic in a search for large prime pairs which was done in the frame of a project for parallel computing together with Járai [58,59]. In these cases, the polynomials are linear. Hence, $C_{f_1\dots f_s}$ can easily be calculated from

$$C_s := \prod_{p>s} \frac{1-s/p}{(1-1/p)^s}.$$

Clearly, $C_1 = 1$, $C_2 = 0.6601\dots$, and $C_3 \approx 0.635$.

In our case, the values of the functions $f_1, \dots, f_s$ are very large. Hence, the logarithms are almost constant in the interval $[a, b]$. So, we used Simpson's rule for the approximation of the integral in (10).

As an example, we consider

$$f_1(n) = (3+30n)2^{38880} + 1 \qquad \text{and} \qquad f_2(n) = (3+30n)2^{38880} - 1.$$

If we plan the search for the interval $[a, b) = [0, 2^{27})$, then we expect

$$\begin{aligned} Q\left(0, 2^{27}\right) &\sim C_{f_1,f_2} \int_0^{2^{27}} \frac{du}{\log f_1(n) \log f_2(n)} \\ &\approx C_{f_1,f_2} \frac{2^{27}}{6}(0.1376769251 + 4 \cdot 0.1374695060 + 0.1374624404)10^{-8} \\ &\approx C_{f_1,f_2} \cdot 0.1845532660, \end{aligned}$$

twin primes. Here,

$$C_{f_1,f_2} = \left(1-\frac{1}{2}\right)^{-2}\left(1-\frac{1}{3}\right)^{-2}\left(1-\frac{1}{5}\right)^{-2} \prod_{p>5} \frac{1-2/p}{(1-1/p)^2} = 20C_2 \approx 13.2032.$$

Hence,

$$Q\left(0, 2^{27}\right) \approx 2.4367.$$

The search for the twin primes consisted then of the following steps.

(1) Since $f_1(n)$ and $f_2(n)$ are coprime to 2, 3, and 5, we started by sieving the 2^{27} values of $f_1(n)$ and $f_2(n)$, respectively, by factors from 7 up to 4400×2^{25}. After sieving, 594866 candidates remained.

(2) These candidates were tested by the probabilistic primality test of Miller and Rabin until a "probable twin prime pair" was found, and this happened already after the test of 55440 candidates.

(3) The "probable twin pair" was tested with exact tests, the -1 case by using a Lucasian type test and the $+1$ case with the use of the test of Brillhart, Lehmer and Selfridge.

The above heuristic suggests that, if we use the sieve with primes $A \le p < B$, then the density of the prime s-tuples is increased by the factor

$$D^{A,B}_{f_1\dots f_s} = \prod_{A\le p<B} \frac{1}{1-(w(p)/p)},$$

and the number of candidates is decreased by this factor. In our cases, these products are reduced to the product

$$D^{A,B}_s = \prod_{A\le p<B} \frac{1}{1-s/p}.$$

These products were calculated in the following way. For $p < L = 1000000$, we did the multiplication, and for the remaining part of the product, we used the approximation $(\log(B)/\log(L))^s$.

This approximation is estimated to have relative error below 0.1%. In the above discussed example, the "twin prime density" $Q(0,2^{27})/2^{27} \approx 2.4367/2^{27} \approx 1.815482974 \times 10^{-8}$ is increased by the factor

$$D_{f_1,f_2}^{7,44000\times 2^{25}} = \prod_{7\le p<44000\times 2^{25}} \frac{1}{1-2/p} = D_2^{7,44000\times 2^{25}} \approx D_2^{7,1000000}\left(\frac{\log 44000\times 2^{25}}{\log 1000000}\right)^2$$
$$\approx 45.86172510 \cdot 4.113596977 \approx 188.6566536,$$

if we sieve with primes in the interval $[A,B) = [7, 44000 \times 2^{25})$. Hence, after sieving, we expect $\approx 2^{27}/188.6566536 \approx 711439.1432$ remaining numbers and an increased "twin prime density" $\approx 188.6566536 \cdot 1.815482974 \times 10^{-8} \approx 3.425029425 \times 10^{-6}$. Testing 55440 numbers, we expect $55440 \times 3.425029425 \times 10^{-6} \approx 0.1899$ twin primes. In 1994, we did searches for the following five sequences:

$$(3+30h)2^{38880} \pm 1,$$
$$(5775+30030h)2^{19380+1} \pm 1,$$
$$(5775+30030h)2^{5040+1} \pm 1,$$
$$(5775+30030h)2^{4980+1} \pm 1,$$
$$(21945+30030h)2^{5056+1} \pm 1.$$

Table 2 compares the results of sieves with their expected values. In Table 3, we compare the computed number of primes and twins with their expected number.

Table 2.

Exponent	Range	Sieve Limit	After Sieve	Expected
38880	$0 \le h < 2^{27}$	2^{35}	947738	949087
19380 + 1	$0 \le h < 2^{27}$	1000×2^{25}	223401	223641
5040 + 1	$0 \le h < 2^{28}$	1000×2^{25}	449119	447601
4980 + 1	$0 \le h < 2^{28}$	1000×2^{25}	448181	447601
5056 + 1	$0 \le h < 2^{28}$	8000×2^{25}	349954	349641

Table 3.

Exponent	Tested	Prime	Expect.	Twin	Expect.
38880	55440	99	102.6	1	0.1899
19380 +1	182488	598	585.3	0	1.878
5040 +1	449119	5452	5510	68	67.6
4980 +1	448181	5646	5564	60	69.1
5056 +1	215000	2819	2855	31	37.9

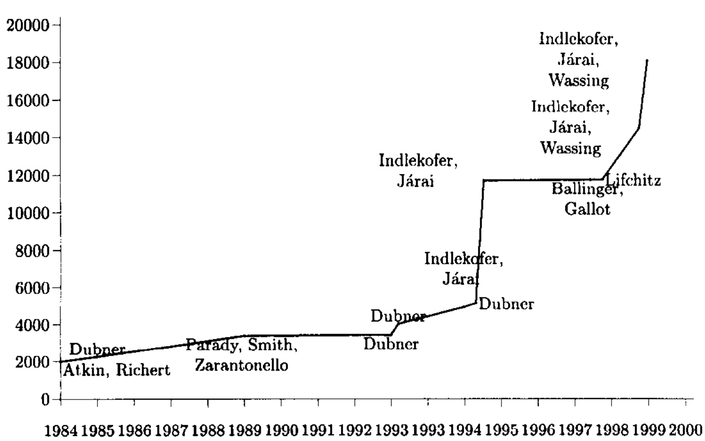

Figure 1. Twin prime records.

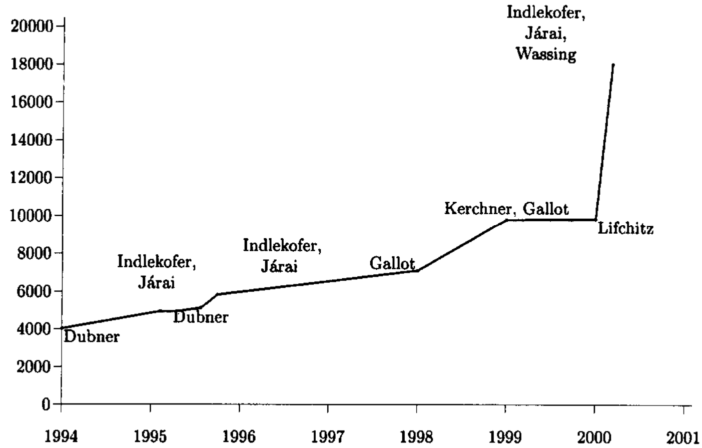

Figure 2. Sophie Germain primes.

Our search for primes and large Sophie Germain primes (i.e., primes p such that $2p + 1$ is a prime, too) were performed in the *Arbeitsgruppe Zahlentheorie* at the University of Paderborn, Germany in the frame of a project for parallel computing in computational number theory. The "world records" we could obtain may be seen from the diagrams of Figures 1 and 2.

REFERENCES

1. J.F. Gauss, *Gesammelte Werke, Vol. 10*, Teubner, Leipzig, (1917).
2. G.H. Hardy and S. Ramanujan, The normal number of prime factors of a number n, *Quart. Journ. Math. Oxford* **40**, 76–92 (1917).
3. P. Turán, On the theorem of Hardy and Ramanujan, *Journ. London Math. Soc.* **9**, 274–276 (1934).
4. P.D.T.A. Elliott, *Probabilistic Number Theory. I: Mean Value Theorems*, Springer-Verlag, (1979); *Probabilistic Number Theory. II: Central Limit Theorems*, Springer-Verlag, (1980).
5. P. Erdős and M. Kac, On the Gaussian law of errors in the theory of additive functions, *Proc. Nat. Acad. Sci. U.S.A.* **25**, 206–207 (1939).
6. P. Erdős and M. Kac, The Gaussian law of errors in the theory of additive number-theoretic functions, *Amer. J. Math.* **62**, 738–742 (1940).
7. P. Erdős, On the density of some sequences of numbers III, *Journ. London Math. Soc.* **13**, 119–127 (1938).
8. P. Erdős and A. Wintner, Additive arithmetical functions and statistical independence, *Amer. Journ. Math.* **61**, 713–721 (1939).
9. J. Kubilius, *Probabilistic Methods in the Theory of Numbers*, Transl. Math. Monographs, Amer. Math. Soc., Providence, RI, (1964).
10. B.V. Levin and N.M. Timofeev, On the distribution of values of additive functions, *Acta Arithmetica* **26** (4), 333–364 (1974/75).
11. A. Bakštys, On limit distribution laws for multiplicative arithmetical functions, *I. Litovsk. Mat. Sb.* (in Russian) **8**, 5–20 (1968).
12. J. Galambos, On the distribution of strongly multiplicative functions, *Bull. London Math. Soc.* **3**, 307–312 (1971).
13. B.V. Levin, N.M. Timofeev and S.T. Tuliaganov, The distribution of the values of multiplicative functions, *Litovsk. Mat. Sb.* **13** (1), 87–100 (1973); English translation, *Math. Trans. Acad. Sci. Lithuanian SSR* **13** (1973).
14. V.M. Zolotarev, On a general theory of multiplication of independent random variables, *Izv. Akad. Nauk* **142** (4), 788–791 (1962); *Soviet Math. (Amer. Math. Soc. Transl.)* **3**, 166–170 (1962).
15. K.F. Roth, Sur quelques ensembles d'entiers, *C.R. Acad. Sci. Paris* **234**, 388–390 (1952).
16. E. Szemerédi, On sets of integers containing no four terms in arithmetic progression, *Acta Math. Acad. Sci. Hung.* **20**, 89–104 (1969).
17. E. Szemerédi, On sets of integers containing no k element in arithmetical progressions, *Acta Arith.* **27**, 199–245 (1975).
18. H. Fürstenberg, Ergodic behaviour of diagonal measures and a theorem of Szemerédi on arithmetic progressions, *J. d'Analyse Math.* **31**, 204–256 (1977).
19. H. Fürstenberg and Y. Katznelson, An ergodic Szemerédi theorem for commuting transformations, *J. d'Analyse Math.* **34**, 275–291 (1978).

20. G.H. Hardy and J.E. Littlewood, Some problems in "Partitio Numerorum" III: On the expression of a number as a sum of primes, *Acta Math.* **44**, 1–70 (1923).
21. P.T. Bateman and R.A. Horn, A heuristic asymptotic formula concerning the distribution of prime numbers, *Math. Comp.* **16**, 363–367 (1962).
22. A.G. Postnikov, *Introduction to Analytic Number Theory*, Transl. of Math. Monographs, Amer. Math. Soc., (1988).
23. K.-H. Indlekofer, Limiting distributions and mean-values of multiplicative arithmetical functions, *Journal für Reine und Angewandte Mathematik* **328**, 116–127 (1981).
24. H. Diamond and P. Erdős, Multiplicative functions whose values are uniformly distributed in $(0, \infty)$, In *Proc. Queen's Number Theory*, (Edited by P. Ribenboim), (1979); Queens papers, *Pure and Appl. Math.*, Queen's Univ., Kingston, Ont., 329–378 (1980).
25. H. Delange, Sur les fonctions arithmétiques multiplicatives, *Ann. Scient. Éc. Norm. Sup.* 3^e *série t.* **78**, 273–304 (1961).
26. E. Wirsing, Das asymptotische Verhalten von Summen über multiplikative Funktionen, II, *Acta Math. Acad. Sci. Hung.* **18**, 411–467 (1967).
27. G. Halász, Über die Mittelwerte multiplikativer zahlentheoretischer Funktionen, *Acta Math. Acad. Sci. Hung.* **19**, 365–403 (1968).
28. K.-H. Indlekofer, Gleichgradige Summierbarkeit bei verallgemeinerten Momenten additiver Funktionen, *Arch. Math.* **49**, 508–512 (1987).
29. A. Wintner, *Eratosthenian Averages*, Waverly Press, Baltimore, MD, (1943).
30. H. Daboussi and K.-H. Indlekofer, Two elementary proofs of Halász's theorem, *Math. Zeitschrift* **209**, 43–52 (1990).
31. K.-H. Indlekofer, Remarks on an elementary proof of Halász's theorem, *Lietuvos Matem. Rinkinys* **33** (4), 417–423 (1993).
32. W. Schwarz and J. Spilker, *Arithmetical Functions*, London Math. Soc. Lecture Note Series, Cambridge Univ. Press, (1994).
33. P.D.T.A. Elliott, Mean value theorems for multiplicative functions bounded in mean α-power, $\alpha > 1$, *J. Australian Math. Soc. (Series A)* **29**, 177–205 (1980).
34. H. Daboussi, Sur les fonctions multiplicatives ayant une valeur moyenne non nulle, *Bull. Soc. Math. France* **109**, 183–205 (1981).
35. K.-H. Indlekofer, A mean-value theorem of multiplicative arithmetical function, *Math. Z.* **172**, 255–271 (1980).
36. K.-H. Indlekofer, On multiplicative arithmetical functions, *Coll. Math. Soc. János Bolyai* **34**, 731–748 (1981).
37. K.-H. Indlekofer, Cesáro means of additive functions, *Analysis* **6**, 1–24 (1986).
38. L.J. Mordell, On Ramanujan's empirical expansions of modular functions, *Proc. Camb. Phil. Soc.* **19**, 117–124 (1917).
39. P. Deligne, La conjecture de Weil, I., *Publ. Math. I.H.E.S.* **43**, 273–307 (1974).
40. R.A. Rankin, Contributions to the theory of Ramanujan's function $\tau(n)$ and similar arithmetical functions, II, *Proc. Camb. Phil. Soc.* **35**, 357–372 (1939).
41. M. Ram Murty, The Ramanujan τ-function in Ramanujan revisited, In *Proc. Centenary Conf.*, Urbana-Champaign, IL, 1987, (Edited by G.E. Andrews *et al.*), pp. 269–288 Academic Press, London, (1988).
42. P.D.T.A. Elliott, *Duality in Analytic Number Theory*, Cambridge Tracts in Mathematics, Cambridge University Press, (1997).
43. D.H. Lehmer, Ramanujan's function $\tau(n)$, *Duke Math. J.* **10**, 483–492 (1943).
44. J.-P. Serre, Quelques applications du théorème de densité de Chebotarev, *Publ. Math. I.H.E.S.* **54**, 123–201 (1982).
45. H. Prüfer, Neue Begründung der algebraischen Zahlentheorie, *Math. Ann.* **94**, 198–243 (1925).
46. E.V. Novoselov, Some formulae connected with a reduced residue system, *Dokl. Akad. Nauk SSSR* **143**, 1274–1277 (1962); English translation, *Soviet Math. Dokl.* **3** (1962).
47. E.V. Novoselov, Topological theory of divisibility of integers, *Elabuzh. Gos. Ped. Inst. Uchen. Zap.* (in Russian) **8**, 3–23 (1960).
48. E.V. Novoselov, Integration on a bicompact ring and its applications to number theory (in Russian), *Izv. Vyssh. Uchebn. Zaved. Mat.* **3** (22), 66–79 (1961).
49. E.V. Novoselov, Foundations of classical analysis and of the theory of analytic functions in a polyadic domain (in Russian), *Izv. Vyssh. Uchebn. Zaved. Mat.* **5** (36), 71–88 (1963).
50. E.V. Novoselov, A new method in probabilistic number theory, *Izv. Akad. Nauk SSSR Ser. Mat.* **28**, 307–364 (1964); English translation, *Amer. Math. Soc. Transl.* **52** (2) (1966).
51. W. Schwarz and J. Spilker, Eine Anwendung des Approximationssatzes von Weierstrass-Stone auf Ramanujan-Summen, *Nieuw. Arch. Wisk.* **19** (3), 198–209 (1971).
52. E. Landau, Über die Äquivalenz zweier Hauptsätze der analytischen Zahlentheorie, *Sitzungsbericht der Kaiserlichen Akad. der Wiss. in Wien, Math. Naturw.* 1202^a, 1–16 (1911).
53. K.-H. Indlekofer, On some spaces of arithmetical functions, *I. Analysis Math.* **18**, 203–221 (1992).
54. L. Gillman and M. Jerison, *Rings of Continuous Functions*, Springer-Verlag, Heidelberg, (1976).

55. H. Fürstenberg, *Recurrence in Ergodic Theory and Combinatorial Number Theory*, Princeton Univ. Press, (1981).
56. M. Kac, *Statistical Independence in Probability, Analysis and Number Theory*, The Carus Math. Monog., (1959).
57. M.F. Jones, M. Lal and W.J. Blundon, Statistics on certain large primes, *Math. Comp.* **21**, 103–107 (1967).
58. K.-H. Indlekofer and A. Járai, Largest known twin primes, *Math. Comp.* **65**, 427–428 (1996).
59. K.-H. Indlekofer, Largest known twin primes and Sophie Germain primes, *Math. Comp.* **68**, 1317–1324 (1999).
60. G.J. Babu, *Probabilistic Methods in the Theory of Arithmetic Functions, Lectures in Math., Volume 2*, Macmillan of India, Delhi, (1978).
61. P.T. Bateman and R.A. Horn, Primes represented by irreducible polynomials in one variable, In *Theory of Numbers, Proc. Symp. Pure Math., Vol. VIII*, pp. 119–132, Amer. Math. Soc., Providence, RI, (1965).
62. H. Daboussi, Charactérisation des fonctions multiplicatives p. p. B^λ à spectre non vide, *Ann. Inst. Fourier (Grenoble)* **30** (3), 141–166 (1980).
63. P. Deligne, Sur les fonctions arithmétiques multiplicatives, *Ann. Scient. Éc. Norm. Sup.* 3[e] *série t.* **78**, 273–304 (1961).
64. P. Erdős and K.-H. Indlekofer, Multiplikative Funktionen auf kurzen Intervallen, *Journal für Reine und Angewandte Mathematik* **381**, 148–160 (1987).
65. J. Fehér, Über die Eindeutigkeits, Zulässigkeits- und (mod 1) Eindeutigkeitsmengen $\mathbb{R}$-additiver Funktionen, *Annales Univ. Sci. Budapest, Sect. Comp.* **14**, 33–37 (1994).
66. J. Fehér, On integer valued multiplicative and additive arithmetical functions, *Annales Univ. Sci. Budapest, Sect. Comp.* **14**, 39–45 (1994).
67. J. Fehér, K.-H. Indlekofer and L.L. Stacho, On sets of uniqueness for completely additive arithmetic functions, *Analysis* **16**, 405–415 (1996).
68. J. Galambos, Limit distribution of sums of (dependent) random variables with applications to arithmetical functions, *Z. Warsch. und. verw. Gebiete* **18**, 261–270 (1971).
69. J. Galambos, Distribution of additive and multiplicative functions, In *The Theory of Arithmetic Functions, Proceedings of Conf. at Western Michigan Univ.*, 1971, Volume 251, pp. 127–139, Springer Lecture Notes-Mathematics, Berlin, (1972).
70. J. Galambos and K.-H. Indlekofer, Additive functions vanishing outside a given set of primes. Part I: Limiting distribution on short intervals, *Publ. Math. Debrecen* **40**, 211–217 (1992).
71. J. Galambos, K.-H. Indlekofer and I. Kátai, A renewal theorem for random walks in multidimensional time, *Trans. Amer. Math. Soc.* **300**, 759–769 (1987).
72. K.-H. Indlekofer, Remark on a theorem of G. Halász, *Arch. Math.* **36**, 145–151 (1980).
73. K.-H. Indlekofer, Some remarks on almost-even and almost-periodic functions, *Arch. Math.* **37**, 353–358 (1981).
74. K.-H. Indlekofer, Properties of uniformly summable multiplicative functions, *Periodica Math. Hung.* **17**, 143–161 (1986).
75. K.-H. Indlekofer, Limiting distributions and mean-values of complex-valued multiplicative functions, *Prob. Theory and Math. Stat.* **1**, 547–552 (1986).
76. K.-H. Indlekofer, Über Grenzverteilungen multiplikativer Funktionen mit logarithmischen Momenten, *Lit. Math. Sbornik* **26**, 435–446 (1986).
77. K.-H. Indlekofer, Über verallgemeinerte Momente additiver Funktionen, *Monatshefte Math.* **103**, 121–132 (1987).
78. K.-H. Indlekofer, Über Verallgemeinerungen der Turán-Kubilius Ungleichung, *Acta Arith.* **52**, 67–73 (1989).
79. K.-H. Indlekofer, Limit laws and moments of additive functions in short intervals, *Coll. Math. Soc. J. Bolyai* Number Theory, Budapest **51**, 193–220 (1989).
80. K.-H. Indlekofer, Limiting distributions of additive functions in short intervals, *Acta Math. Acad. Sci. Hung.* **56**, 11–22 (1990).
81. K.-H. Indlekofer, A new method in probabilistic number theory, *Mathematics and Its Applications*, Probability Theory and Applications **80**, 299–308 (1992).
82. K.-H. Indlekofer and I. Kátai, Momente additiver Funtionen auf der Folge $\{p+1\}$, *Lietuvos Mat. Rinkinys* **28**, 669–679 (1988).
83. K.-H. Indlekofer and I. Kátai, Generalized moments of additive functions, *J. Number Theory* **32**, 281–288 (1989).
84. K.-H. Indlekofer and I. Kátai, Multiplicative functions with small increments, I, *Acta Math. Hung.* **55**, 97–101 (1990).
85. K.-H. Indlekofer and I. Kátai, Multiplicative functions with small increments, II, *Acta Math. Hung.* **56**, 159–164 (1990).
86. K.-H. Indlekofer and I. Kátai, Multiplicative functions with small increments, III, *Acta Math. Hung.* **58**, 121–132 (1991).
87. K.-H. Indlekofer and I. Kátai, On the distribution of translates of additive functions, *Acta Math. Hung.* **61**, 343–356 (1993).
88. K.-H. Indlekofer and N.M. Timofeev, A mean value theorem for multiplicative functions on the set of shifted primes, *The Ramanujan Journal* **2**, 153–165 (1998).

89. K.-H. Indlekofer and N.M. Timofeev, Estimates for multiplicative functions on the set of shifted primes, *Acta Math. Hungar.* **81**, 195–221 (1998).
90. K.-H. Indlekofer and N.M. Timofeev, On some subsets of the set of shifted primes, *Publ. Math. Debrecen* **52**, 429–468 (1998).
91. I. Kátai, On the distribution of arithmetical functions on the set of prime plus one, *Compositio Math.* **19**, 278–289 (1968).
92. I. Kátai, On the distribution of arithmetical functions, *Acta Math. Hung.*, 69–87 (1969).
93. I. Kátai, Distribution of digits of primes in q-ary canonical form, *Acta Math. Hung.* **47**, 341–359 (1986).
94. I. Kátai, Distribution of q-additive functions, *Mathematics and its Applications, Probability Theory and Applications* **80**, 309–318 (1992).
95. J. Maddox, *Elements of Functional Analysis*, Cambridge Univ. Press, (1970).
96. J.-L. Mauclaire, *Intégration et Théorie des Nombres*, Hermann, Paris, (1986).
97. M. Ram Murty, Some Ω-results for Ramanujan's τ-function, In *Proc. Third. Mat. Science Conf., Mysore, 1981, Volume 938*, pp. 122–137, Lecture Notes in Math., Springer-Verlag, (1982).
98. P. Ribenboim, *The New Book of Prime Number Records*, Springer-Verlag, (1996).
99. A. Schönhage, A.F.W. Grotefeld and E. Vetter, *Fast Algorithms: A Multitape Turing Machine Implementation*, B.I. Wissenschafsverlag, Mannheim, (1994).
100. N.M. Timofeev, The Turán-Erdős hypothesis on the distribution of the values of additive functions on the sequences of shifted primes, *Acta Arithm.* **58**, 113–131 (1991).
101. N.M. Timofeev, Stable law for additive arithmetic functions, *Matem. Zametki* **37** (4), 465–472 (1985).
102. P. Turán, Über einige Verallgemeinerungen eines Satzes von Hardy und Ramanujan, *Journ. London Math. Soc.* **11**, 125–133 (1936).
103. K.-H. Indlekofer and A. Jarai, Some world records in computational number theory, *Leaflets in Mathematics*, 49–56 (1998).