There are three appendices: (1) Elementary properties of symmetric matrices over fields. (2) The geometry of metric spaces as another expression of the theory of quadratic forms. (3) Modules and ideals in quadratic fields $\mathbf{Q}(\sqrt{\Delta})$ and their norm forms. This is helpful for the understanding of the Euler products occurring in Chapter Four.

## REFERENCES

1. M. Eichler, *Quadratische Formen und orthogonale Gruppen*, 2nd ed., Springer-Verlag, Berlin, Heidelberg, New York, 1974.

2. ——, *Einführung in die Theorie der Algebraischen Zahlen und Funktionen*, Birkhäuser-Verlag, Basel and Stuttgart, 1963=*Introduction to the theory of algebraic numbers and functions*, Academic Press, New York and London, 1966.

3. E. Freitag, *Siegelsche Modulfunktionen*, Springer-Verlag, Berlin, Heidelberg, New York, 1983.

MARTIN EICHLER

BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 18, Number 2, April 1988

0273-0979/88 $1.00 + $.25 per page

*Arithmetic functions and integer products*, by P. D. T. A. Elliott. Grundlehren der Mathematischen Wissenschaften, vol. 272, Springer-Verlag, New York, Berlin, Heidelberg and Tokyo, 1985, xv + 461 pp., $64.00. ISBN 0-387-96094-5

*Introduction to arithmetical functions*, by Paul J. McCarthy, Springer-Verlag, New York, Berlin, Heidelberg and Tokyo, 1986, vi + 365 pp., $35.50. ISBN 0-387-96262-X

**1. The theory of numbers: its great conjectures.** Problems in number theory have fascinated generations of professional and amateur scientists. Still today mathematicians are attracted to number theory because its history has brought so many conjectures. Some, like the Riemann Hypothesis, stated in 1859 (see §2), and the Goldbach conjecture, which goes back to 1742 (see §6), have yet to be proven. Others, thanks to the ingenuity of contemporary mathematicians or to highly sophisticated computer methods, have been resolved: such is the case of the Mertens conjecture (see §5), which was proven false by Odlyzko and te Riele [**39**] in 1983, some 86 years after it was stated.

Many problems in number theory involve arithmetical functions. Our intent here is to present a survey of (what we feel are) the most significant results in the theory of arithmetical functions, thereby leading us into a review of the books of McCarthy and Elliott. Though our presentation obviously cannot be exhaustive, our objective is to display most of the classical arithmetical functions (those which "made history") and to introduce the reader to the methods used by mathematicians to analyze their behavior. The two books under review are mainly concerned with results and methods in elementary and analytic number theory, though the second assumes some knowledge of probabilistic number theory; thus our survey will reflect the development of arithmetical functions only in these three areas.

**2. The Prime Number Theorem: the first significant result.** Already in 300 B.C., Euclid was aware of the fundamental theorem of arithmetic ("given $n \in \mathbf{N}$, there exist $r \in \mathbf{N}$ and primes $q_1 < q_2 < \cdots < q_r$ such that $n$ is uniquely written as $n = q_1^{\alpha_1} \cdot q_2^{\alpha_2} \cdots q_r^{\alpha_r}$ for some positive integers $\alpha_i$") and proved that there exist infinitely many primes. Nevertheless, until a few centuries ago, number theory progressed by strictly elementary methods. But when, in the 18th century, Legendre and Gauss claimed that $\pi(x)$, the number of primes up to $x$, behaves somewhat like $x/(\log x)$—they were essentially stating what is known today as the *Prime Number Theorem* (from here on denoted by PNT), i.e.,

$$\lim_{x\to\infty} \frac{\pi(x)}{x/(\log x)} = 1$$

—more powerful methods such as analysis made their entrance in the race for solving major number theory problems. Gauss knew that $\mathrm{Li}(x) \overset{\text{def}}{=} \int_2^x dt/(\log t)$ was asymptotic to $x/(\log x)$, and he suggested, using a table of primes up to $3,000,000$, that $\pi(x)$ is asymptotic to $\mathrm{Li}(x)$. He died before one could obtain a proof of his conjecture. It took a little more than a century before it could be proven: it was finally established independently by Hadamard and de la Vallée Poussin in 1896. This was certainly the first significant achievement in the area of analytic number theory. It was indeed so deep that an elementary proof of the PNT was only obtained in 1949 when Erdős [**13**] and Selberg [**42**] separately published proofs of it.

In their proof of the PNT, both Hadamard and de la Vallée Poussin used what we now call the *Riemann zeta function*, defined by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}. \tag{1}$$

This series obviously converges for any real $s > 1$. Euler was familiar with it. For instance, he noticed that, for $s > 1$,

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}, \tag{2}$$

where the infinite product extends over all primes. Relation (2) is commonly called the Euler identity. In 1859, essentially a century later, Riemann, in a famous ten-page paper [**40**], considered the series $\sum_{n=1}^{\infty} 1/n^s$ for complex $s$, and extended the function $\zeta$ to the whole complex plane, showing by analytic continuation that, except for a pole of order 1 at $s = 1$, $\zeta(s)$ is analytic in $\mathbf{C}$. He proved the famous functional equation (already known to Euler for real $s$)

$$\zeta(1-s) = 2(2\pi)^{-s} \cos(\pi s/2)\Gamma(s)\zeta(s), \tag{3}$$

deduced from it that $\zeta(-2n) = 0$ for all integers $n \geq 1$, and further claimed that the only other solutions to $\zeta(s) = 0$ satisfy $\mathrm{Re}(s) = 1/2$. This statement about the distribution of the zeros of the Riemann zeta function is known as the *Riemann Hypothesis* (from now on denoted by RH). Relation (2) being also true for all $s \in \mathbf{C}$ such that $\mathrm{Re}(s) > 1$, it is easy to prove that $\zeta(s+it) \neq 0$ if $\mathrm{Re}(s) > 1$. From (3) it follows that $\zeta(s+it) \neq 0$ if $\mathrm{Re}(s) < 0$. Hence besides the trivial zeros $s = -2n$, $n \geq 1$, all the zeros $\rho = \beta + i\gamma$ of $\zeta$ must satisfy

$0 \le \beta \le 1$. Hadamard and de la Vallée Poussin proved that $\zeta(1+it) \neq 0$ for all real $t$ (which by (3) also means that $\zeta(it) \neq 0$), a fact which turned out to be equivalent to the PNT. They actually proved that

$$\pi(x) = \mathrm{Li}(x) + O(x\exp(-c\sqrt{\log x})) \tag{4}$$

(here $f(x) = O(g(x))$ means that there exists a constant $C > 0$ such that $|f(x)| < C|g(x)|$ if $x$ is sufficiently large), for some positive constant $c$.

The size of the error term in (4) depends on the location of the zeros of the zeta function. For instance, if it could be proved that $\zeta(s) \neq 0$ for all $s$ such that $\mathrm{Re}(s) \ge \theta$ for some $\frac{1}{2} < \theta < 1$, then we would have, for any fixed $\varepsilon > 0$, $\pi(x) = \mathrm{Li}(x) + O(x^{\theta+\varepsilon})$. Assuming RH, von Koch [**34**] proved that

$$\pi(x) = \mathrm{Li}(x) + O(x^{1/2}\log x). \tag{5}$$

The breakthrough initiated by Riemann confirmed the close interaction between the theory of functions of one complex variable and the theory of arithmetical functions. This connection is further studied in §5.

**3. The group of arithmetical functions.** It can easily be shown that the PNT is equivalent to the statement $\psi(x) \sim x$, where $\psi(x) = \sum_{n \le x} \Lambda(n)$, $\Lambda$ being the von Mangoldt function defined on the positive integers by $\Lambda(n) = \log p$ if $n = p^\alpha$ for a certain prime $p$ and $\alpha \in \mathbf{N}$, and $\Lambda(n) = 0$ otherwise. (Here and in what follows $f(x) \sim g(x)$ means that $\lim_{x\to\infty} f(x)/g(x) = 1$.) The von Mangoldt function is a particular example of an *arithmetical function*, that is, a complex-valued function defined on the natural numbers. *Arithmetic function* and *number-theoretic function* are synonyms of *arithmetical function.* Although it is not explicit in the definition, such a function should have some kind of "arithmetic flavor" in the sense that the value associated with the integer $n$ should somehow reflect or depend on the arithmetic structure of $n$.

More than 3000 years ago the Pythagoreans were studying *perfect numbers*, that is those positive integers which are equal to the sum of their proper divisors, or in other words the solutions of the equation $\sigma(n) = 2n$, where $\sigma(n)$ stands for the sum of the divisors of $n$. For instance, 6, 28, 496 and 8128 are perfect numbers. Euclid proved that every integer $2^{m-1}(2^m - 1)$, where $2^m - 1$ is a prime number, is perfect and moreover that all even perfect numbers are of that form. As of today, no odd perfect number is known.

The arithmetical function $\sigma$ is a member of a large class of arithmetical functions known as the multiplicative functions. A function $f$ is said to be *multiplicative* if $f(mn) = f(m)f(n)$ whenever $(m,n) = 1$. From this definition it follows that if $f$ is not identically zero, then $f(1) = 1$. Moreover each multiplicative function $f$ is entirely determined by its values on prime powers, that is

$$f(n) = f\Big(\prod_{p^\alpha \| n} p^\alpha\Big) = \prod_{p^\alpha \| n} f(p^\alpha). \tag{6}$$

(Here $p^\alpha \| n$ means that $p^\alpha$ divides $n$, but $p^{\alpha+1}$ does not.) Let $a$ be a fixed complex number, and define $I_a(n) = n^a$ for each $n \ge 1$; clearly $I_a$ is a multiplicative function. It is also a *totally* (or *completely*) *multiplicative function*: $f$ is such a function if $f(mn) = f(m)f(n)$ for all $m, n \in \mathbf{N}$. The *divisor function*

$d$ defined by $d(n) = \sum_{d|n} 1$ is multiplicative, but not totally multiplicative. The functions $d$ and $\sigma$ are particular cases of the more general multiplicative function $\sigma_a(n) = \sum_{d|n} d^a$, where $a$ is a fixed complex number. Since $\sigma_a$ is multiplicative, we obtain from (6) that

$$\sigma_a(n) = \prod_{p^\alpha \| n} (1 + p^a + p^{2a} + \cdots + p^{\alpha a}),$$

which in the case $a = 0$ yields a neat formula for the divisor function, namely $d(n) = \prod_{p^\alpha \| n}(\alpha + 1)$.

If we denote by $A$ the set of all arithmetical functions $f$ such that $f(1) \neq 0$ and by $M$ its subset of multiplicative functions, it can be shown that $M$ is a subgroup of $A$ with respect to the *Dirichlet convolution* $*$:

$$(f * g)(n) = \sum_{d|n} f(d)g(n/d).$$

One easily verifies that $(A, *)$ and $(M, *)$ are abelian groups, the identity element being the function $E$ defined as $E(1) = 1$ and $E(n) = 0$ if $n > 1$. Here $d = 1 * 1$ and $\sigma = 1 * I$, with $I = I_1$ and $1(n) = 1$ for all $n$. The *Moebius function* $\mu$, defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n \text{ is divisible by a square } > 1, \\ (-1)^r & \text{if } n \text{ is the product of } r \text{ distinct primes,} \end{cases}$$

plays a central role in the group $A$: Indeed $\mu * 1 = E$ and hence $\mu^{-1} = 1$; this means that if $f = 1 * g$, or equivalently if $f(n) = \sum_{d|n} g(d)$, then $g = \mu * f$, that is $g(n) = \sum_{d|n} \mu(n/d)f(d)$. This last formula is known as the *Moebius inversion formula* and is used in deriving various identities involving arithmetical functions. The function $\mu$ is also an important actor in the play of sieve methods (see Halberstam and Richert [**21**]).

Of major interest in number theory is the *Euler totient function* $\phi$ defined by $\phi(n) = \#\{m \leq n : (m, n) = 1\}$. One can prove that $\phi \in M$ and that

$$\phi(n) = n \prod_{p|n} (1 - 1/p) = n \sum_{d|n} \mu(d)/d.$$

Therefore $\phi = \mu * I$. Multiplying both sides by the function 1 yields the relation $\phi * 1 = I$ or equivalently $\sum_{d|n} \phi(d) = n$, a very useful identity. The important congruence $a^{\phi(m)} \equiv 1 \pmod{m}$, where $a, m \in \mathbf{N}$ and $(a, m) = 1$, was discovered by Euler some 250 years ago. In the late seventies, this apparently simple result allowed mathematicians to build a code which is almost impossible to break even though the key is made public (see for instance Rivest, Shamir and Adleman [**41**]).

A further generalization of the divisor function is the following: for a fixed $k \in \mathbf{N}$, let $d_k(n)$ denote the number of representations of $n$ as a product of $k$ positive integers. Clearly $d(n) = d_2(n)$. Moreover

$$d_k = 1 * \cdots * 1, \tag{7}$$

the product being taken $k$ times. This function is studied in §§4 and 5.

Another important subset of $M$ is the set of specially multiplicative functions. Consideration of these functions arises naturally in the theory of modular forms (see Apostol [1]). A function $f \in M$ is said to be *specially multiplicative* if there exists $g \in M$ such that for all $m, n \in \mathbf{N}$ one has

$$f(mn) = \sum_{d|(m,n)} f(m/d)f(n/d)g(d).$$

The function $\sigma_a$ defined above is such a function. The *Ramanujan tau-function*, denoted $\tau$ and defined by

$$x\prod_{k=1}^{\infty}(1-x^k)^{24} = \sum_{n=1}^{\infty}\tau(n)x^n \qquad (|x|<1)$$

is also a specially multiplicative function. The numbers $\tau(n)$ appear as Fourier coefficients of a certain modular function (see Apostol [1, Chapter 6]).

Associated to $f \in M$ is the *Dirichlet series* $D_f(s)$ where

$$D_f(s) = \sum_{n=1}^{\infty}\frac{f(n)}{n^s} = \prod_p\left(1+\frac{f(p)}{p^s}+\frac{f(p^2)}{p^{2s}}+\cdots\right).$$

Note that if $f$ is totally multiplicative then

$$\sum_{n=1}^{\infty}\frac{f(n)}{n^s} = \prod_p\left(1-\frac{f(p)}{p^s}\right)^{-1}.$$

Finally observe that, given any $f, g \in A$, the identity

$$(8)\quad D_{f*g}(s) = \sum_{n=1}^{\infty}\frac{(f*g)(n)}{n^s} = \left(\sum_{n=1}^{\infty}\frac{f(n)}{n^s}\right)\left(\sum_{n=1}^{\infty}\frac{g(n)}{n^s}\right) = D_f(s)D_g(s),$$

which reveals a close connection between Dirichlet series and Dirichlet convolution, can be used to prove various identities (see Ayoub [2]).

Before ending this section, let us mention that *additive functions*, those satisfying $f(mn) = f(m) + f(n)$, whenever $(m, n) = 1$, also shed interesting information on the multiplicative structure of the positive integers. Obviously $\log n$ is such a function, two others being $\omega$ and $\Omega$, where $\omega(n)$ and $\Omega(n)$ denote respectively the number of different prime factors of $n$ and the total number of prime divisors of $n$. Note that if $f \in M$ and $f(n) \neq 0$ for all $n$, then $\log f$ is additive. Furthermore, a function $f$ is said to be *totally* (or *completely additive*) if $f(mn) = f(m) + f(n)$ for all $m, n \in \mathbf{N}$. Additive functions are fully studied in probabilistic number theory (see §7).

**4. Elementary methods leading to asymptotic results.** Given $f \in A$, it is natural to inquire about the behavior of $S_f(N) \overset{\text{def}}{=} \sum_{n\le N} f(n)$, when $N$ is large. In the case of $\Lambda$, the answer lies in the statement of the PNT, that is,

$$(9)\qquad S_\Lambda(N) = \psi(N) \sim N,$$

when $N \to \infty$. In a sense, (9) means that the "average order" of $\Lambda(n)$ is 1. This motivates the following definition: an arithmetical function $f$ is said to have a *mean value* $M(f)$ if $N^{-1}S_f(N)$ tends to a limit when $N$ tends to infinity, in which case we set $M(f) = \lim_{N\to\infty} S_f(N)/N$.

There are standard techniques relying on real analysis for estimating $S_f(N)$. One of them lies in a theorem due to Wintner which states that if two arithmetical functions $f$ and $g$ satisfy

$$f = 1 * g \tag{10}$$

and if $\sum_{n=1}^{\infty} g(n)/n^s$ converges absolutely at $s = 1$, then $M(f)$ exists and is equal to $\sum_{n=1}^{\infty} g(n)/n$. For a proof, see De Koninck and Mercier [**5**, p. 120]. Note that, because of (8), relation (10) is equivalent to

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \zeta(s) \sum_{n=1}^{\infty} \frac{g(n)}{n^s},$$

which reflects a type of relation satisfied by several well-known arithmetic functions. For example, one can apply Wintner's Theorem to $f(n) = \mu^2(n)$ and easily obtain that the density of the set of square-free integers is $6/\pi^2$.

One can generalize Wintner's theorem by stating that if $f$ and $g$ are arithmetical functions satisfying $f = 1^k * g$ (here $1^k = 1 * \cdots * 1$, the product being taken $k$ times) for some positive integer $k$ and if $\sum_{n=1}^{\infty} g(n)/n$ converges absolutely, then, as $n \to +\infty$,

$$\sum_{n \le N} f(n) = (1 + o(1)) \frac{1}{(k-1)!} \left( \sum_{n=1}^{\infty} \frac{g(n)}{n} \right) N \log^{k-1} N;$$

(here $f(x) = o(g(x))$ means that $\lim_{x \to \infty} f(x)/g(x) = 0$). The proof is elementary (see De Koninck and Mercier [**5**, p. 149]). This formula can be applied to the divisor function. Indeed, since $d = 1^2 * E$, it follows that

$$\sum_{n \le N} d(n) = (1 + o(1)) N \log N. \tag{11}$$

More generally, since by (7), $d_k = 1^k * E$, one can show that

$$\sum_{n \le N} d_k(n) = (1 + o(1)) \frac{1}{(k-1)!} N \log^{k-1} N,$$

a minor step towards the study of the Dirichlet divisor problem (see §5).

Several elementary methods have been created in studying number-theoretic functions. As an example, we describe one which is due to Dirichlet. For the sake of comparing different approaches with the same "client", we consider once more the divisor function and write successively

$$\begin{aligned} \sum_{n \le N} d(n) &= \sum_{n \le N} \sum_{ab = n} 1 = \sum_{ab \le N} 1 = \sum_{a \le N} \sum_{b \le N/a} 1 = \sum_{a \le N} [N/a] \\ &= \sum_{a \le N} N/a + \sum_{a \le N} ([N/a] - N/a) = N \sum_{a \le N} 1/a + O(N) \\ &= N \log N + O(N), \end{aligned}$$

where we used the fact that

$$\sum_{a \le N} 1/a = \log N + O(1); \tag{12}$$

(here $[x]$ stands for the largest integer not exceeding $x$). We have thus proven slightly more than (11) since we have now obtained information about the

size of the error term. Essentially, though, our result is no deeper than (12). In order to estimate more precisely $S_d(N)$, Dirichlet introduced a geometric approach. He observed that $\sum_{ab\le N} 1$ represents the number of lattice points located in the first quadrant on or under the hyperbola $xy = N$. He then argued that

(13)
$$\sum_{n\le N} d(n) = \sum_{ab\le N} 1 = 2\sum_{a\le\sqrt{N}} [N/a] - [\sqrt{N}]^2$$
$$= 2\sum_{a\le\sqrt{N}} N/a + 2\sum_{a\le\sqrt{N}} ([N/a] - N/a) - (\sqrt{N} + ([\sqrt{N}] - \sqrt{N}))^2.$$

Using the more accurate formula $\sum_{a\le N} 1/a = \log N + \gamma + O(1/N)$, where $\gamma = -\int_0^\infty e^{-x}\log x\,dx = 0.577\ldots$ stands for the *Euler constant*, he obtained

$$\sum_{n\le N} d(n) = N\log N + (2\gamma - 1)N + O(\sqrt{N}). \tag{14}$$

The method of Dirichlet is known as the "*hyperbola method*" and can be used in a variety of estimates (see Ayoub [**2**, Theorem 7.7]). It is important (at least historically!) to observe that relation (14) represents only the beginning of a series of improvements in the evaluation of $\sum_{n\le N} d(n)$. Indeed, let

$$\Delta(N) = \sum_{n\le N} d(n) - N\log N - (2\gamma - 1)N. \tag{15}$$

How large is $\Delta(N)$? We have shown, by (14), that $\Delta(N) = O(\sqrt{N})$. To further improve upon this estimate of $\Delta(N)$, more powerful tools are needed, such as complex integration. But first, we consider additive functions.

The global behavior of additive functions is generally easier to study than that of the multiplicative ones. Indeed, if $f$ is additive, then

$$\sum_{n\le N} f(n) = N\sum_{p\le N}\frac{f(p)}{p} + N\sum_{p^\alpha\le N}\sum_{\alpha\ge 2}\frac{f(p^\alpha) - f(p^{\alpha-1})}{p^\alpha}$$
$$+ O\Big(\sum_{p^\alpha\le N}\sum_{\alpha\ge 1} |f(p^\alpha) - f(p^{\alpha-1})|\Big), \tag{16}$$

and in most cases, the first two terms on the right-hand side of (16) are easy to estimate while the $O$-term is small compared to the first two. For example, one can easily obtain from (16) that, with

$$B = \gamma + \sum_p (1/p + \log(1 - 1/p)),$$

$$\sum_{n\le N} \omega(n) = N(\log\log N) + BN + O(N/\log N). \tag{17}$$

Analyzing the local behavior of additive functions presents a different challenge: this is one of the topics of probabilistic number theory (see §7).

**5. Complex integration.** If it is known that the mean value of a particular arithmetical function $f$ exists, then one can use its associated Dirichlet series $D_f(s) = \sum_{n=1}^{\infty} f(n)/n^s$ to calculate $M(f)$. Indeed, using the Mellin transform of $S_f(t)$, the existence of $M(f)$ implies that, for $\mathrm{Re}(s) > 1$ and as $s \to 1^+$,

$$D_f(s) = s\int_1^{\infty} \sum_{n<t} f(n)t^{-s-1}\,dt = (1+o(1))M(f)s\int_1^{\infty} t^{-s}\,dt$$
$$= (1+o(1))M(f)\frac{s}{s-1}.$$

Hence $M(f) = \lim_{s\to 1}(s-1)D_f(s)$.

Complex integration can also be used to investigate the behavior of $\sum_{n\le t} f(n)$. The standard approach is as follows. If $a > 0$, then

$$\frac{1}{2\pi i}\int_{a-i\infty}^{a+i\infty} x^s s^{-1}\,ds \overset{\text{def}}{=} \frac{1}{2\pi i}\lim_{T\to\infty}\int_{a-iT}^{a+iT} x^s s^{-1}\,ds \tag{18}$$
$$= \begin{cases} 0 & \text{if } 0 \le x < 1, \\ 1 & \text{if } x > 1. \end{cases}$$

Now, given $f \in A$, suppose that its associated Dirichlet series $D_f(s)$ converges absolutely for $\mathrm{Re}(s) > \alpha$, where $\alpha$ is a certain positive real number. Arguing formally, we obtain (assuming that $x$ is not an integer and $a > \alpha$)

$$\frac{1}{2\pi i}\int_{a-i\infty}^{a+i\infty} D_f(s)x^s s^{-1}\,ds = \sum_{n\le x} f(n)\frac{1}{2\pi i}\int_{a-i\infty}^{a+i\infty}(x/n)^s s^{-1}\,ds$$
$$+ \sum_{n>x} f(n)\frac{1}{2\pi i}\int_{a-i\infty}^{a+i\infty}(x/n)^s s^{-1}\,ds.$$

Using (18), one can easily obtain that the last two integrals are equal to $2\pi i$ and 0 respectively. This means that

$$\sum_{n\le x} f(x) = \frac{1}{2\pi i}\int_{a-i\infty}^{a+i\infty} D_f(s)x^s s^{-1}\,ds, \tag{19}$$

provided that $a > \alpha = \alpha_f$, the so-called abscissa of convergence of $D_f(s)$. The inversion formula (19) is often called in the literature *Perron's formula* (for a detailed proof of it, see Titchmarsh [**44**, p. 300]). The process of obtaining information about $\sum_{n\le x} f(n)$ using the behavior of $\sum_{n=1}^{\infty} f(n)/n^s$ is what we call a *Tauberian theorem for Dirichlet series.* Now the integral on the right side of (19) is not always easy to compute. But when $f$ is multiplicative, the corresponding $D_f(s)$ is often "simple"—as is the case for $f = d$, $\mu^2$, $\phi$, or $\sigma$ (see Ayoub [**2**])—in which case the integral in (19) can be calculated quite accurately. For instance, since $\sum_{n=1}^{\infty} d(n)/n^s = \zeta^2(s)$, we have from (19) that

$$\sum_{n\le x} d(n) = \frac{1}{2\pi i}\int_{a-i\infty}^{a+i\infty} \zeta^2(s)x^s s^{-1}\,ds, \tag{20}$$

provided $a > 1$. The function $\zeta^2(s)x^s s^{-1}$ is analytic in the whole plane except for two poles at $s = 0$ and $s = 1$. Now using Cauchy's theorem and estimates

of $\zeta(\sigma+it)$ for $\sigma<1$, one can proceed to move the line integral in (20) to the left of $\sigma=1$, picking up on the way the residue of $\zeta^2(s)x^s s^{-1}$ at $s=1$, which is equal to $x\log x+(2\gamma-1)x$. This accounts for the first two terms already obtained in (14). Various estimates of $\zeta(s)$ allowed mathematicians to further improve upon the size of $\Delta(x)$ (defined in (15)). For instance Kolesnik [35] proved that $\Delta(x)=O(x^{35/108+\varepsilon})$. It is conjectured that

$$\Delta(x)=O(x^{1/4+\varepsilon}).$$

The problem of obtaining the best upper bound for $\Delta(x)$ is a particular case of the general "Dirichlet divisor problem": let

$$\Delta_k(x)=\sum_{n\le x} d_k(n)-x\cdot P_{k-1}(\log x)$$

be the error term in the asymptotic formula for $\sum_{n\le x} d_k(n)$; what is the size of $\Delta_k(x)$? (Here $P_{k-1}(\log x)$ is a polynomial of degree $k-1$ in $\log x$ which is equal to the residue of $\zeta^k(s)x^s s^{-1}$ at $s=1$.)

Let $M(x)=\sum_{n\le x}\mu(n)$; it is well known that $M(x)=o(x)$, an estimate which is equivalent to the PNT. On the other hand, it has so far been impossible to prove that there exists $\lambda>0$ such that $M(x)=O(x^{1-\lambda})$. Under RH one could obtain $M(x)=O(x^{1/2+\varepsilon})$ for any $\varepsilon>0$ (see Ivić [28, p. 47]). In 1897, Mertens conjectured that $|M(x)|\le\sqrt{x}$ for all $x\ge 1$. In view of the fact that $\sum_{n=1}^{\infty}\mu(n)/n^s=1/\zeta(s)$ and using the methods described in this paragraph, it becomes clear that the estimation of $M(x)$ depends on the location of the zeros of the Riemann zeta function in the critical strip $0<\sigma<1$. Using an old method of Landau adapted by Grosswald [19]), one can show that there exists a constant $c\in]0,1[$ such that each of the two inequalities $M(x)\gtrless\pm c\sqrt{x}$ occur infinitely often as $x\to\infty$. But unfortunately by classical methods one cannot show (so far!) that $c$ can be chosen greater than 1 and thus contradict the Mertens conjecture. Nevertheless, by using computer methods, Odlyzko and te Riele [39] were able to disprove the Mertens conjecture.

**6. Functions from additive number theory.** Let $S$ be a set of integers. Additive number theory is concerned with the problem of determining if a given integer $n$ can be expressed as a sum of (possibly a restricted number of) elements of $S$, and, if so, in how many ways. Hence to any such problem, one can associate an arithmetical function $f(n)=f(n;S,k)$ which counts the number of ways that $n$ can be expressed as a sum of $k$ elements of $S$. So, for each such problem, one is generally interested by two types of queries: #1. Is $f(n)>0$ for all $n\in\mathbf{N}$? #2. What is the size of $f(n)$?

To show how popular this theory is, we mention the famous Goldbach conjecture which states that every even integer greater than 4 is expressible as a sum of two primes; this is the case when $S=P$, the set of all primes, and $k=2$. No one yet has been able to prove or disprove this conjecture, although it is generally believed to be true. Even if in this case no one can give an answer to question #1, some are already speculating about question #2. Indeed it was conjectured by Hardy and Littlewood [22] in 1922 that

for this problem the corresponding function $f(n) = f(n; P, 2)$ satisfies

$$f(n) = (1 + o(1))\frac{2cn}{\log^2 n} \prod_{p|n;\, p\neq 2} \frac{p-1}{p-2},$$

as $n \to \infty$, where $c = \prod_{p>2}(1 - (p-1)^{-2})$.

We come back to the general setting and consider the case where $S = \mathbf{N}$ and $k$ is unspecified: this gives the partition function $p(n)$ which counts the number of partitions of $n$ into natural numbers. The study of the partition function uses a combination of combinatorial and analytic methods. This is due essentially to the nice properties of the power series $\sum_{n=0}^{\infty} p(n)x^n$ (here it is convenient to define $p(0) = 1$). Indeed, just as Dirichlet series proved to be the natural tool for the study of multiplicative functions, for most problems of additive number theory, power series yield the proper setup for analyzing the properties and the behavior of the corresponding functions $f$. In the case of the partition function, we first observe that

$$F(x) \overset{\text{def}}{=} \sum_{n=0}^{\infty} p(n)x^n = \prod_{k=1}^{\infty} (1 - x^k)^{-1}.$$

This formal identity, besides providing various combinatorial identities (see Ayoub [**2**]), is the starting point in the process of finding an asymptotic estimate for $p(n)$. In 1918, Hardy and Ramanujan [**24**] showed, using analytic methods, that

$$p(n) = (1 + o(1))((4\sqrt{3}\, n)^{-1} \exp(\pi\sqrt{2n/3})).$$

The best estimates concerning the size of $p(n)$ for large $n$ are obtained by the use of the "circle method" due to Hardy (other important contributors being Davenport, Littlewood, Mordell, Rademacher, Ramanujan and Vinogradov). This method is too complex to explain in such a short exposition, but let us only mention the general idea. First, by Cauchy's Theorem, we have that

$$p(n) = \frac{1}{2\pi i} \int_C \frac{F(x)}{x^{n+1}}\, dx,$$

where $C$ is a simple closed contour around the origin lying inside the unit circle. The ingenuity of this method is to replace the contour of integration along $|x| = 1$ by a path consisting of a sequence of abutting arcs inside the unit circle chosen close enough to allow a fairly good approximation of $F(x)$ by simple functions along the new path of integration.

In ending this brief discussion on additive number theory, we mention two problems, one solved and one unsolved, which portray how difficult it is to relate the additive structure of an integer to its multiplicative one. The first of these is a conjecture stated by Erdős and Mirsky [**16**] in 1952 and which says that there exist infinitely many integers $n$ such that $d(n) = d(n+1)$. Many have been baffled over this problem, but, in 1984, Heath-Brown [**25**], adding a new idea to an argument of Spiro [**43**] finally proved the conjecture; he actually obtained much more, namely that there exists $c > 0$ such that $\#\{n \le x\colon d(n) = d(n+1)\} > cx/\log^7 x$ for $x$ sufficiently large. Our second problem is the already famous "*abc* conjecture": Let $a, b, c$ be relatively prime integers such that $a+b = c$; then, given $\varepsilon > 0$, there exists $K = K(\varepsilon) > 0$ such

that $\max(|a|,|b|) < K(\prod_{p|abc} p)^{1+\varepsilon}$. This conjecture is very deep: indeed, one can show that if it were true then Fermat's Last Theorem, which says that, for each integer $n > 2$, the equation $x^n + y^n = z^n$ has no integral solution with $xyz \neq 0$, would also be true for $n$ sufficiently large (see Vojta [**46**]).

**7. Probabilistic number theory.** So far we have been mainly concerned with the global behavior of arithmetical functions. Investigating their local behavior and in particular the distribution of the values of multiplicative or additive functions is in general a much more difficult problem. A first indication to that effect comes from observing that usually, given a function $f$, multiplicative or additive, the behavior of the sequence $f(1), f(2), f(3), \ldots$ is very erratic. This is perhaps not so surprising. Indeed, if the sequence $(f(n))_{n\in\mathbf{N}}$ were smooth in the sense that it is a nondecreasing sequence of real numbers, then one could show that there exists a constant $c \geq 0$ such that $f(n) = c(\log n)$ (if $f$ is additive) or $f(n) = n^c$ (if $f$ is multiplicative). This was proven by Erdős [**12**] in 1946 in the case of additive functions. His proof was ingenious but entirely elementary. It is almost ironic that it was only seven years later that Lambek and Moser [**37**], apparently unaware of Erdős' result, stated and proved the analogous result for multiplicative functions. But their proof was much simpler. In 1958, Erdős proved that the condition of monotonicity can be somewhat relieved: he showed that, if $f$ is additive and $\liminf_{n\to\infty}(f(n+1) - f(n)) = 0$, then $f \in \mathscr{L}$, where $\mathscr{L} = \{f\colon \mathbf{N} \to \mathbf{R}$ such that $f(n) = c\log n$ for all $n \in \mathbf{N}$, for some $c \in \mathbf{R}\}$. In 1970, Kátai [**33**] established another conjecture of Erdős, namely that, if $f$ is additive and, as $x \to \infty$, $x^{-1}\sum_{n\leq x} |f(n+1) - f(n)| \to 0$, then $f \in \mathscr{L}$. This was also proven by Wirsing [**48**].

Even though most multiplicative and additive functions oscillate erratically, when one studies the distribution of their values, it turns out that several questions can be formulated and answered using ideas and methods of probability theory. Hence one can say that *probabilistic number theory* is the study of the distribution of the values of multiplicative or additive arithmetical functions. The mere use of probabilistic methods in number theory can be interpreted as saying that one is working in the area of probabilistic number theory. Perhaps this second "definition" is the best; indeed, does the PNT belong to elementary number theory, analytic number theory or probabilistic number theory? In fact, it belongs to all three of them! This particular example also shows that the three areas are not disjoint. In any event, probabilistic number theory is very young; to quote Elliott [**10**], it "may be viewed as a Twentieth-Century Sport".

If $f$ is multiplicative and nonzero, then $\log f$ is additive; hence it generally is sufficient to study the distribution of values of additive functions. To better understand how probabilistic number theory was born, let us consider the function $\omega$ introduced in §3. From (17), one can easily say that the average value of $\omega(n)$ in the interval $[1, N]$ is $\log\log N$ or, in probabilistic terms, that the expected value of $\omega(n)$ is $\log\log n$. On the other hand, clearly $\liminf_{n\to\infty} \omega(n) = 1$ and furthermore one can show that

$$\limsup_{n\to\infty} \omega(n)\log\log n/\log n = 1.$$

Hence the function $\omega(n)$ oscillates often between 1 and $(\log n)/(\log\log n)$. Therefore is is natural to inquire to what extent the function $\omega(n)$ deviates from its average value $\log\log n$ for most integers $n$ in a given interval $[1, N]$. The first nontrivial answer to this question was given in 1917 by Hardy and Ramanujan [**23**]. They proved that, given any positive $\psi(n)$ such that $\lim_{n\to\infty}\psi(n) = +\infty$, the number of integers $n \leq N$ such that $|\omega(n) - \log\log N| > \psi(N)\sqrt{\log\log N}$ is $o(N)$. This means that, for almost all positive integers $n \leq N$, $\omega(n)$ deviates from $\log\log N$ by no more than $\psi(N)\sqrt{\log\log N}$. Their argument, although arithmetical, was essentially an analogue of the probability-theoretic law of large numbers. This was further confirmed in 1934 by Turán [**45**], who gave a new proof of Hardy and Ramanujan's result. His proof was based on the elementary estimate $\sum_{n\leq N}(\omega(n) - \log\log N)^2 \leq c_3 N\log\log N$. A similar argument holds if one considers $\Omega$ instead of $\omega$. Examining Turán's proof, one can recognize an argument (unknown to Turán at that time) of Tchebycheff in the theory of probability.

In their 1917 paper, Hardy and Ramanujan introduced the notion of "normal order" of an arithmetical function $f$: given $\varepsilon > 0$, if the set of integers $n$ for which $|f(n) - g(n)| \geq \varepsilon g(n)$ is of density zero, where $g(n)$ is an "elementary" and increasing function, then $f(n)$ is said to have *normal order* $g(n)$. For example, $\omega(n)$ and $\Omega(n)$ both have normal order $\log\log n$. Necessary and sufficient conditions for an additive function to have a normal order are given in the book of Elliott [**10**]. On the other hand, it was proven by Birch [**3**] that the only multiplicative functions $f$ having a normal order are those defined by $f(n) = n^c$, where $c \in \mathbf{R}$.

Let $\mathscr{P}$ be a property satisfied by certain integers. By $N_x(n;\mathscr{P})$, we mean the number of positive integers $n$ not exceeding $x$ which satisfy property $\mathscr{P}$. For each $x \geq 1$, we define the frequency $\nu_x(n;\mathscr{P})$ as the number $[x]^{-1}N_x(n;\mathscr{P})$. Approximately five years after Turán's paper came out, Erdős and Kac [**14, 15**] confirmed the importance of probability theory in the study of number-theoretic problems: using the central limit theorem of probability theory and elementary arithmetic methods such as the sieve of Eratosthenes, they proved that, given a real-valued *strongly additive function* $f$ (that is, an additive function such that $f(p^\alpha) = f(p)$ for all primes $p$ and $\alpha \in \mathbf{N}$) such that $|f(p)| \leq 1$ and for which

$$B(x) = \sum_{p\leq x}\left(\frac{f(p)^2}{p}\right)^{1/2} \to \infty$$

as $x \to \infty$, then

$$\lim_{x\to\infty}\nu_x\left(n; \frac{f(n) - A(x)}{B(x)} \leq z\right) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{z} e^{-w^2/2}\,dw,$$

where $A(x) = \sum_{p\leq x} f(p)/p$. Clearly $\omega$ is such a function.

One can say that the central problem in studying the distribution of the values of additive functions $f(n)$ is to investigate when functions $\alpha(x)$ and $\beta(x) > 0$ may be found such that the frequencies

$$\nu_x(n; f(n) - \alpha(x) \leq z\beta(x)) \tag{21}$$

possess a limiting distribution as $x \to \infty$. The famous Erdős-Wintner theorem corresponds to the choice $\beta(x) = 1$ and $\alpha(x) = 0$ and states that an additive function $f$ possesses a limiting distribution if and only if the three series

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

converge. The proof of this theorem appeared in several steps in the literature. For a simple proof, see Galambos and Kátai [**17**]. Necessary and sufficient conditions for the existence of a distribution function for multiplicative functions are given in Galambos and Szüsz [**18**].

A major tool in establishing the limiting behavior of the frequencies (21) is the Turán-Kubilius inequality which can be stated as follows: There exists an absolute constant $c$ such that, for all $N \in \mathbf{N}$, one has

$$\sum_{n\le N} |f(n) - A(N)|^2 \le cND(N)^2 \tag{22}$$

uniformly for all complex-valued additive functions $f$, where

$$A(N) = \sum_{p\le N} \frac{f(p)}{p}$$

and

$$D(N) = \left( \sum_{p^k \le N} |f(p^k)|^2/p^k \right)^{1/2} \ge 0.$$

In his book *Probabilistic number theory* I, Elliott [**9**] gave a proof of (22) with $c \le 32$ with an argument yielding $\limsup c \le 2$. Recently, Hildebrand [**26**] showed that, as $N \to \infty$, $c \to 3/2$.

Mean value theorems have great importance in probabilistic number theory. Here is why. Let $f$ be a real additive function. Using the theory of Fourier transforms, one has that the characteristic function $\Phi_N(t)$ (defined for real $t$) of the distribution function $F_N(z) = \nu_N(n; f(n) \le z)$ is given by

$$\Phi_N(t) = \int_{-\infty}^{\infty} e^{itz}\, dF_N(z) = N^{-1} \sum_{n\le N} e^{itf(n)}.$$

If there exists some function $\Phi(t)$ continuous at $t = 0$ such that $\lim_{N\to\infty} \Phi_N(t) = \Phi(t)$, then $F_N(z)$ converges to some distribution function $F(z)$ at each of its points of continuity, and hence $\Phi(t)$ is the characteristic function of $F(x)$. Thus the problem of investigating the asymptotic behavior of $N^{-1}\sum_{n\le N} g(n)$, where $g$ is a complex-valued multiplicative function bounded by 1, becomes very important. On this matter, Delange [**6**] proved, in 1961, that necessary and sufficient conditions for the existence of a nonzero mean value for a multiplicative function $g$ bounded by 1 are that $\sum_p (g(p) - 1)/p$ converges and that, for all primes $p$, $\sum_{k=0}^{\infty} g(p^k)/p^k \ne 0$. The problem of characterizing those multiplicative functions $g$ bounded by 1 such that $M(g)$ exists and is equal to zero was solved by Wirsing [**47**] in 1967, but only for the case of real-valued functions. One year later, Halasz [**20**] solved the problem in the case of complex-valued functions. One can read more about this in the book of Elliott [**9**]. Other books relevant to the study of probabilistic number theory are the books of Kac [**29**] and of Kubilius [**36**].

**8. The books of McCarthy and Elliott.** McCarthy's purpose is to give "contemporary results" concerning arithmetical functions. He focuses his attention on special topics and carries the reader "beyond the point at which textbooks abandon the subject". Although the author does not present his material in that order, we see three main topics being dealt with:

1. *Multiplicative functions*: Their elementary properties (including the fact that $(A, *, \cdot)$ is a ring), their generating functions and some asymptotic results involving them (such as the hyperbola method described above in §4).

2. *Ramanujan's sums* (that is, for fixed $k \in \mathbf{N}$ and $n \in \mathbf{N}$, the sum of the $n$th powers of the primitive $k$th roots of unity) and how they can be used to count the number of solutions $(x_1, \ldots, x_s)$ of $n \equiv a_1x_1 + \cdots + a_sx_s \pmod{r}$.

3. *Two generalizations*: One is an extension of the Dirichlet convolution: let $K: \mathbf{N} \times \mathbf{N} \to \mathbf{C}$, $f, g \in A$, then define

$$(f *_K g)(n) = \sum_{d|n} K(n,d) f(d) g(n/d);$$

the case $K(n,d) = 1$ if $(d, n/d) = 1$ and 0 otherwise yields the well-known unitary convolution

$$(f \circledast g)(n) = \sum_{d|n;\,(d,n/d)=1} f(d) g(n/d).$$

The other one concerns generalized arithmetical functions $f: P \times P \to \mathbf{C}$, where $P$ is a partially ordered set.

Particularly interesting is the author's presentation of specially multiplicative functions (which we introduced in §3), a subject usually not included in textbooks but nevertheless of great importance in the theory of modular functions.

Although the book does not cover a wide variety of subjects, it is very pleasant to read. On the other hand, it is certainly suited for an undergraduate or beginners' graduate course in number theory: students will be motivated and challenged by some 400 exercises (which, incidentally, fill 128 of the book's 365 pages).

While McCarthy's book is quite elementary and readily accessible to university students, the book of Elliott is much more advanced and is written for specialists. It includes much of the already published work of the author, but it also does contain many new results.

Let $a_1, a_2, \ldots,$ be a sequence of positive integers; then every positive integer $n$ has a product representation

$$n = a_1^{d_1} \cdots a_k^{d_k}, \tag{23}$$

for suitably chosen $k \in \mathbf{N}$ and $d_j \in \mathbf{Z}$. This is one of the important results proved in Elliott's book. "Who cares?" one might say. Actually, many should and many will if they read what follows.

Elliott studies representations of positive integers as products of rationals of a prescribed type and shows how this problem plays a central role in solving several conjectures involving number-theoretic functions. This is one reason for rejoicing. There is another one. In order to derive most of his results, the author combines in a very neat way the ring-theoretic properties of the

integers with methods of elementary functional analysis. Without this original approach, most of the results he produces would still be unobtainable.

Here are two of the conjectures which motivated the subject. As we saw in §7, Erdős [12] proved that, if $f$ is additive and

$$f(n+1) - f(n) \to 0, \quad \text{as } n \to \infty, \tag{24}$$

then $f \in \mathscr{L}$. Notice that condition (24) is essential in the sense that it cannot be replaced, say, by "$f(3n+1) - f(n) \to 0$, as $n \to \infty$". Around 1970, Kátai [31, 32] asked for a characterization of those additive functions which satisfy

$$f(an+b) - f(An+B) \to C, \quad \text{as } n \to \infty, \tag{25}$$

for some integers $a > 0$, $b$, $A > 0$, $B$ and constant $C$. Partial results with $B = 0$ were obtained by Kátai [31, 32], and Mauclaire [38]. In his book, Elliott provides a complete solution to Kátai's problem. More precisely, he proves

THEOREM A. *If $f$ is as above and further if the integers $a > 0$, $b$, $A > 0$, $B$ satisfy $\Delta = aB - Ab \neq 0$, then there is a constant $C$ such that $f(n) = C \log n$ for all $n \in \mathbf{N}$ such that $(n, aA\Delta) = 1$.*

This result follows essentially from a new method introduced by Elliott for quantitatively characterizing real-valued additive functions in terms of their differences $f(an+b) - f(An+B)$. More precisely, in order to prove Theorem A, the author uses a "basic inequality" (somewhat typical of many estimates displayed in the manuscript): "The inequality

$$\sum_{\substack{q \le x \\ (q, aA\Delta)=1}} \frac{1}{q} |f(q) - F(x) \log q|^2 \ll \sup_{x < n \le x^c} \frac{1}{w} \sum_{x < n \le w} |f(an+b) - f(An+B)|^2,$$

with

$$F(x) = \Bigg( \sum_{\substack{x^{1/2} < q \le x \\ (q, aA\Delta)=1}} \frac{f(q)}{q} \Bigg) \Bigg( \sum_{\substack{x^{1/2} < q \le x \\ (q, aA\Delta)=1}} \frac{\log q}{q} \Bigg)^{-1}$$

holds uniformly for all additive functions $f(n)$ for all $x \ge x_0$. Here $x_0, c$ and the implied constant depend at most upon $a, b, A$ and $B$; $q$ denotes a prime-power." (Here $h(x) \ll g(x)$ means that $h(x) = O(g(x))$.) The proof of this estimate, although it uses only elementary techniques including several applications of the Cauchy-Schwarz inequality and the Chinese Remainder Theorem, is very complicated and covers almost 30 pages.

So far, we have mentioned very little about integer products (actually, apart from a few pages, Elliott starts writing about these only in Chapter 15), but here they come. Kátai [30] called a set of uniqueness a sequence $a_1 < a_2 < \cdots$ of positive integers with the property that every real-valued completely additive function which vanishes on each $a_i$ also vanishes identically. Kátai showed that there exists a constant $K > 0$ such that $\{p+1 : p \text{ is prime}\} \cup \{p : p \le K\}$ is a set of uniqueness. His proof was based on a result of Bombieri [4] in the theory of the large sieve. He further conjectured that $\{p+1 : p \text{ is prime}\}$ is a set of uniqueness, that is, that a completely additive function is entirely determined by its values on "shifted primes", a result

which Elliott [8] finally established in 1974. Elliott's proof also used large sieve estimates and various results on the distribution functions of additive functions. In 1976, Indlekofer [27] displayed a large class of sets of uniqueness. Then, in 1978, Wolke [50], and Dress and Volkmann [7] proved, using vector spaces over $\mathbf{Q}$, that in order for a sequence $(a_j)_{j\in\mathbf{N}}$ to be a set of uniqueness, it is necessary and sufficient that every positive integer $n$ have a multiplicative representation

$$n^h = \prod a_{j_i}^{\varepsilon_i} \tag{26}$$

with $\varepsilon_i = \pm 1$ (here $h$ may vary with $n$). With this result, it became clear that uniqueness statements for additive functions are related to statements about multiplicative representations of positive integers (see also Wirsing [49]). Indeed, a careful analysis of the proof of Elliott [8] shows that each positive integer $n$ has a representation

$$n^h = \prod (p_{j_i} + 1)^{\varepsilon_i}, \qquad \varepsilon_i = \pm 1, \tag{27}$$

a particular case of (26). All these results, we believe, motivate a systematic study of "integer products". The product representation (23) portrays one of the many connections between the theory of arithmetical functions and certain problems in algebra. We will only mention here the general set-up used by Elliott in his presentation. Let $a_1, a_2, \ldots$ be a sequence of positive integers. Suppose one wants to show that every positive integer $n$ can be written as in (23). Consider the multiplicative group $\mathbf{Q}^*$ of positive rationals. Let $\Gamma$ denote the subgroup generated by the $a_j$'s. Then form the quotient group $G = \mathbf{Q}^*/\Gamma$. The general procedure consists in proving that (i) $G$ is finitely generated, (ii) $G$ is of bounded order (that is, there is an integer $m$ such that the $m$th power of every element in it is the identity) and (iii) $G$ is trivial. Since every real-valued completely additive function $f$ can be extended in a natural way to $\mathbf{Q}^*$ by defining $f(r/s) = f(r) - f(s)$ for each $r/s \in \mathbf{Q}^*$, Elliott considers a completely additive function as a group homomorphism of $(\mathbf{Q}^*, \cdot)$ into the additive reals $(\mathbf{R}, +)$; but these homomorphisms differ only insofar as they assume values in nonisomorphic groups, and thus the attention is focused on the image groups. This is only the starting point of a general setting which allows the author to use the full power of algebraic methods. Consider now the vector space $\mathbf{C}^m = \mathbf{C} \times \cdots \times \mathbf{C}$ (over the field $\mathbf{C}$). On this space, define the $L^2$ norm by

$$\|y\|_m = \left( \sum_{j=1}^{m} |y_j|^2 \right)^{1/2}.$$

Now let $x$ be a fixed large number and put $s = s(x) = \#\{p^k \le x\}$. Since every complex-valued additive function is entirely determined by its values at the prime powers, one can easily construct a one-to-one correspondence between $\mathbf{C}^{[x]}$ and $\mathbf{C}^{s(x)}$. Define the operator $T\colon \mathbf{C}^{s(x)} \to \mathbf{C}^{[x]}$ by

$$T(f)(n) = \sum_{p^k \| n} f(p^k)(p^k(1 - 1/p))^{-1/2} - \sum_{p^k \le x} f(p^k)((1 - 1/p)/p^k)^{1/2}.$$

Then the Turán-Kubilius inequality (22) can be regarded as a bound for the norm of $T$. Elliott studies the underlying operator $T$. For this problem

and others, he applies several tools of functional analysis. These techniques allow one to consider classical problems involving arithmetical functions with a different approach. In particular, it can be shown that determining the best constant in the Turán-Kubilius inequality is equivalent to finding the spectral radius of a certain operator (see Hildebrand [**26**], Elliott [**11**]).

Finally we observe that, by including a series of 108 exercises and a list of 18 open problems at the end of his manuscript, Elliott makes an effort to reach the graduate student. On the other hand, he further improves upon his presentation by including a kind of update on some of the material published in his two books on probabilistic number theory [**9**, **10**].

What makes a particular subject in mathematics interesting is either the importance of its results or the scope of the methods used to derive them. By his presentation, Elliott shows that the theory of arithmetic functions satisfies both these criteria.

## REFERENCES

1. T. M. Apostol, *Modular functions and Dirichlet series in number theory*, Graduate Texts in Math., No. 41, Springer-Verlag, 1976.

2. R. Ayoub, *An introduction to the analytic theory of numbers*, Amer. Math. Soc., Providence, R.I., 1963.

3. B. J. Birch, *Multiplicative functions with non-decreasing normal order*, J. London Math. Soc. **42** (1967), 149–151.

4. E. Bombieri, *On the large sieve*, Mathematika **12** (1965), 201–225.

5. J.-M. De Koninck and A. Mercier, *Approche élémentaire de l'étude des fonctions arithmétiques*, Presses Univ. Laval, Québec, 1982.

6. H. Delange, *Sur les fonctions arithmétiques multiplicatives*, Ann. Sci. École Norm. Sup. **78** (1961), 273–304.

7. F. Dress and B. Volkmann, *Ensembles d'unicité pour les fonctions arithmétiques additives ou multiplicatives*, C. R. Acad. Sci. Paris Ser. A **287** (1978), 43–46.

8. P. D. T. A. Elliott, *A conjecture of Kátai*, Acta Arith. **26** (1974), 11–20.

9. ——, *Probabilistic number theory*. I, Springer-Verlag, Berlin and New York, 1979.

10. ——, *Probabilistic number theory*. II, Springer-Verlag, Berlin and New York, 1980.

11. ——, *Functional analysis and additive arithmetic functions*, Bull Amer. Math. Soc. (N.S.) **16** (1987), 179–223.

12. P. Erdős, *On the distribution of additive functions*, Ann. of Math. (2) **47** (1946), 1–20.

13. ——, *On a new method in elementary number theory which leads to an elementary proof of the prime number theorem*, Proc. Nat. Acad. Sci. (Washington) **35** (1949), 374–384.

14. P. Erdős and M. Kac, *On the Gaussian law of errors in the theory of additive functions*, Proc. Nat. Acad. U.S.A. **25** (1939), 206–207.

15. ——, *The Gaussian law of errors in the theory of additive number-theoretic functions*, Amer. J. Math. **62** (1940), 738–742.

16. P. Erdős and L. Mirsky, *The distribution of values of the divisor function $d(n)$*, Proc. London Math. Soc. **2** (1952), 257–271.

17. J. Galambos and I. Kátai, *A new proof for the continuity of the limiting distribution of some arithmetical functions*, Proc. Budapest Conference (to appear).

18. J. Galambos and P. Szüsz, *On the distribution of multiplicative arithmetical functions*, Acta Arith. **47** (1986), 57–62.

19. E. Grosswald, *Oscillation theorems of arithmetical functions*, Trans. Amer. Math. Soc. **126** (1967), 1-28.

20. G. Halasz, *Über die Mittelwerte multiplikativer zahlentheoretischer Funktionen*, Acta Math. Sci. Hungar. **19** (1968), 365–403.

21. H. Halberstam and H. E. Richert, *Sieve methods*, Academic Press, New York, 1974.

22. G. Hardy and J. E. Littlewood, *Some problems of partitio numerorum*. III: *On the expression of a number as a sum of primes*, Acta Math. **44** (1922), 1–70.

23. G. H. Hardy and S. Ramanujan, *The normal number of prime factors of a number n*, Quart. J. Math. (Oxford) **48** (1917), 76–92.

24. ——, *Asymptotic formulae in combinatory analysis*, Proc. London Math. Soc. **17** (1918), 75–115.

25. D. R. Heath-Brown, *The divisor function at consecutive integers*, Mathematika **31** (1984), 141–149.

26. A. Hildebrand, *An asymptotic formula for the variance of an additive function*, Math. Z. **183** (1983), 145–149.

27. K. H. Indlekofer, *On sets characterizing additive arithmetical functions*, Math. Z. **146** (1976), 285–290.

28. A. Ivić, *The Riemann zeta function*, John Wiley & Sons, New York, 1985.

29. M. Kac, *Statistical independence in probability, analysis and number theory*, Carus Math. Monographs, No. 12, Math. Assoc. America (distributed by John Wiley and Sons, New York), 1959.

30. I. Kátai, *On sets characterizing number-theoretical functions*, Acta Arith. **13** (1968), 315–320.

31. ——, *Some results and problems in the theory of additive functions*, Acta Sci. Math. Szeged. **30** (1969), 305–311.

32. ——, *On number-theoretical functions*, Colloq. Math. Soc. János Bolyai, 2, North-Holland, Amsterdam, 1970, 133–136.

33. ——, *On a problem of P. Erdős*, J. Number Theory **2** (1970), 1–6.

34. H. von Koch, *Sur la distribution des nombres premiers*, Acta Math. **24** (1901), 159–182.

35. G. Kolesnik, *On the order of $\zeta(\sigma+it)$ and $\Delta(R)$*, Pacific J. Math. **98** (1982), 107–122.

36. J. Kubilius, *Probabilistic methods in the theory of numbers*, Trans. Math. Monographs, vol. 11, Amer. Math. Soc., Providence, R.I., 1968.

37. J. Lambek and L. Moser, *On monotone multiplicative functions*, Proc. Amer. Math. Soc. **4** (1953), 544–545.

38. J. L. Mauclaire, *Sur la régularité des fonctions additives*, Séminaire Delange-Pisot-Poitou, Théorie des Nombres, Paris **15** (1973/74), no. 23.

39. A. M. Odlyzko and H. J. J. te Riele, *Disproof of the Mertens conjecture*, J. Reine Angew Math. **357** (1985), 138–160.

40. B. Riemann, *Über die Anzahl der Primzahlen unter eine gegebenen Grosse*, Monatsh. Preuss. Akad. Wiss. (Berlin) (1859), 671–680.

41. R. Rivest, A. Shamir and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Comm. ACM **21** (1978), 120–126.

42. A. Selberg, *An elementary proof of the prime number theorem*, Ann. of Math. (2) **50** (1949), 305–313.

43. C. Spiro, Ph.D. Thesis, Univ. of Illinois, Urbana, Ill., 1981.

44. E C. Titchmarsh, *The theory of functions*, Oxford University, 1952.

45. P. Turán, *On a theorem of Hardy and Ramanujan*, J. London Math. Soc. **9** (1934), 274–276.

46. P. Vojta, *Diophantine approximations and value distribution theory*, Lecture Notes in Math., Springer-Verlag, 1987.

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

48. ——, *Characterization of the logarithm as an additive function*, Proc. Sympos. Pure Math., vol 20, Amer. Math. Soc., Providence, R.I., 1971, pp. 375–381.

49. ——, *Additive functions with restricted growth on the numbers of the form $p+1$*, Acta Arith. **37** (1981), 345–357.

50. D. Wolke, *Bemerkungen über Eindeutigkeitmengen additiver Funktionen*, Elem. Math. **33** (1978), 14–16.

JEAN-MARIE DE KONINCK