followed by a very detailed consideration of the Riemann and Lindelöf hypotheses, and finally a chapter on the approximate functional equation. There are seven appendices covering such general topics as Fourier theory, the gamma function and the Phragmén–Lindelöf theorem.

The author's knowledge both of the history of his subject and modern developments is impressive and a reader who has studied the book in detail will find that he has acquired a deeper appreciation of the theory. Some parts of the chapter on the Riemann hypothesis have been asterisked to indicate that they require a background of algebraic geometry. These are undoubtedly the most difficult parts of the book, while at the same time being the most valuable for any mathematician intending to carry out research in the area.

At the ends of each chapter and of several of the appendices there are numerous exercises. There are a number of misprints and minor errors, which should be easily corrected.

R. A. RANKIN

KOBLITZ, N., *A course in number theory and cryptography* (Graduate Texts in Mathematics 114, Springer-Verlag, Berlin–Heidelberg–New York 1987) viii + 208 pp. 3 540 96576 9, DM 74.

As a human activity, cryptography has a long and fascinating history, going back probably almost as far as writing itself. As a branch of mathematics, however, it is a newcomer. And while mathematical and statistical ideas have been used for some time for breaking secret codes, the use of number theoretic methods for the construction of codes is a very recent development. It has enabled teachers and grant applicants to sell number theory as an area of mathematics with applications, and has brought an unprecedented amount of computing power and expertise into the subject. (The fact that much of this power is directed towards finding good factoring algorithms is somewhat ironic, for if really good factoring algorithms were found, most number-theory-based crypto-systems would be fatally weakened, and practical applications of number theory to cryptography would largely disappear!) This brings us to the main difficulty of regarding cryptography as a respectable branch of mathematics: its dearth of theorems on the strength of cryptosystems. While number theory can be used to construct cyphers, we have no proof of their security, and so no real idea at present whether number theory is to have a lasting place in cryptography.

The text under review gives us, in the author's typically clear style, firstly the number theory we need, followed by chapters on simple cryptosystems, public key ciphers, primality testing and factoring. Finally there is a chapter on elliptic curves and their use in cryptosystems and factorization. The book is carefully written, is self-contained, has plenty of exercises (and some nice quotations). With the exception of the final chapter, I would place the level of the book at upper undergraduate rather than postgraduate, and certainly below the level of other texts in Springer's Graduate Texts in Mathematics series (including others by Koblitz). This applies particularly to most of the material in chapter three, some of which would make interesting excercises for a first linear algebra course. This level is perhaps determined more by the mathematical immaturity of the subject, however, rather than by the author's choice of material.

The book concentrates on number theoretic applications to cryptography, and does not try to give a comprehensive introduction to cryptography. Thus one time pads, and block ciphers such as the Data Encryption Standard are not mentioned. As a result, it may be difficult for the reader to appreciate the revolutionary nature of public key cryptosystems. Also, the definitions of one-way and trapdoor functions are confused. No distinction is made between functions whose inverse is always difficult to compute and those having a "trapdoor" where special extra information makes the inverse easy to calculate. Nevertheless, the book contains much material of interest to anyone wanting to broaden the scope of an elementary number theory course, and as such is to be thoroughly recommended.

Finally, mention should be made of the small, ill-spaced typeface used in the book, which can only be described as an assault on the eye. Although it was prepared by the author in camera-

ready form, Springer must bear some responsibility for allowing it to mar the appearance of their celebrated series.

C. J. SMYTH

CHAMPENEY, D. C., *A handbook of Fourier theorems* (Cambridge University Press 1987) xii + 185 pp. 0 521 26503 7, £25.

This handbook is intended to assist postgraduates and research workers in the physical sciences, particularly communications and electronic engineering, who have met Fourier analysis and its applications in a non-rigorous way, and wish to find out the exact conditions under which particular results can be used. Its major part therefore consists of rigorous statements of important results in Fourier theory, together with explanatory comments and examples. This is preceded by chapters which introduce necessary mathematical ideas, for example Lebesgue integration, the inequalities of Hölder and Minkowski, and notions such as absolute and uniform continuity, and dominated and mean convergence. No proofs are given in the book, nor precise references for proofs of individual theorems, but there is a comprehensive bibliography accompanied by a summary detailing those books which cover the results of particular chapters.

As one would expect, the coverage of material is selective. There are a great many results on ideas associated with convolutions and products, and on convergence of Fourier series and integrals; the latter include results on convergence in L^p, and on (C, 1) and Abel summability, together with many standard counterexamples. Fourier integrals are treated over some nine chapters, which include one on power spectra and Wiener's theorem, and three on generalised functions and their transforms; these are followed by two chapters listing analogous results for Fourier series and generalised Fourier series.

I have one or two minor reservations over notation, for example it seems perverse to use $*$ for complex conjugate as well as convolution, and I feel that a direct definition of measure would have been more illuminating than one defining it as the integral of a characteristic function, provided this function is in L, when no properties of functions in L have been proved. However let me stress the virtues, an excellent commentary throughout, with cross references and a good index, very good coverage in its chosen areas, and glimpses of other topics such as the Hilbert transform and almost periodic functions. As a reference book written in modern style, this handbook will have considerable value to a mathematician as well as to an engineer. It is beautifully printed and I found very few misprints.

PHILIP HEYWOOD

HARTE, R., *Invertibility and singularity for bounded linear operators* (Marcel Dekker Inc., New York and Basel, 1987) xii + 590 pp. 0 8247 7754 9, $119.50.

This textbook provides not only a most comprehensive introduction to functional analysis but, in addition, contains accounts of Fredholm theory, multiparameter spectral theory and the complicated ideas of Joseph Taylor.

The various kinds of "singularity" which prevent an operator from being invertible are studied in detail. The text concentrates on two major theorems: namely, the open mapping theorem and the Hahn–Banach theorem. Completeness is introduced and several types of nonsingularity are studied. In particular their algebraic and topological characteristics are looked at and the transmission of these to subspaces, quotients and products. The Hahn–Banach theorem is followed by the dual space construction. It is indicated how nonsingularity behaves under the process of taking the dual. Two major constructions are described: namely, the extension of classical complex analysis to the vector-valued case and the "enlargement" of a normed space.