solved on rectangular, or at least conceptually rectangular domains. One would expect to see an example of how a domain can be broken up for solving a PDE using finite elements on an unstructured mesh. The chapter ends with a short discussion of multilevel ILU preconditioners. This again is restricted to SPD matrices.

All in all, *Computer solution of large linear systems* would make a fine reference book for engineers, computer scientists, and mathematicians working with large systems. It is most useful for those working with symmetric positive definite systems. The book presents a large number of useful algorithms, along with the important theory governing their behavior. It also does a wonderful job of citing other sources where one can fill in the details.

Brian Suchomel
Department of Computer Science
and Engineering
University of Minnesota
Minneapolis, Minnesota 55455

9[11L05, 11L40, 65C10, 94A60, 94B05]—*Character sums with exponential functions and their applications*, by Sergei Konyagin and Igor Shparlinski, Cambridge University Press, New York, NY, 1999, viii+163 pp., 23 1/2 cm, hardcover, $49.95

The main theme of this monograph is the distribution of the powers of an integer g with $1 < g < p$ modulo a prime p. Character sums with exponential functions in the argument form the most important tool in the analysis. Many of the problems considered here are motivated by applications, and a good part of the book is devoted to applications. The book collects known results, most of them of fairly recent origin, but also presents new theorems not published before. One stated aim of the book is to stimulate further research, and this goal has certainly been reached, for instance through the many open problems that the authors pose along the way.

The first two chapters set the stage via introductory remarks and auxiliary results. Chapters 3 to 6 are devoted to the core of the theory, namely bounds for character sums with exponential functions in the argument and related bounds for Gaussian sums. Chapters 7 to 10 deal with number-theoretic applications; for instance, to multiplicative translates of sets modulo p and to class numbers of cyclotomic fields. Chapter 11 considers the important problem of the occurrence of given strings in digit expansions of rational numbers, which is connected with the Blum-Blum-Shub pseudorandom bit generator in cryptography. Applications to linear congruential pseudorandom numbers, in particular the question of the existence of good multipliers, are treated in Chapter 12. Chapters 13 and 14 are more of number-theoretic interest, whereas the distribution theorems in Chapter 15 allow very interesting applications to a "pseudo-randomized" version of the QuickSort algorithm. In the last three chapters, the treatment of upper bounds for the dimension of BCH codes is of particular relevance from the viewpoint of applications.

Harald Niederreiter