on pp. 160–161 the statement of Theorem 97 is interrupted by Table 9.3.

H. N.

17[62-01, 62J10, 62Kxx, 65Fxx].—RICHARD M. HEIBERGER, *Computation for the Analysis of Designed Experiments*, Wiley Series in Probability and Mathematical Statistics—Applied Probability and Statistics, Wiley, New York, 1989, xv + 683 pp., 24 cm. Price $59.95.

ANOVA (analysis of variance) programs form an important part of statistical software packages. This book discusses in great detail how ANOVA programs are constructed and how their components work. Broader issues in the design of software systems for statistical applications are also treated quite extensively. The book is divided into five parts which cover statistically designed experiments, programming systems, least squares and ANOVA, the interpretation of design specifications, and the analysis of statistically designed experiments.

The treatment of these topics is very much oriented towards application and computation, with little emphasis on the development of the underlying theory. Most concepts are introduced by examples and few words are lost on basic ideas like Latin squares or block designs. An introductory chapter on the theoretical underpinnings would have done no harm. The author gives a lot of useful advice on programming style and on the handling of program systems on the user level. The book contains a generous supply of programs in FORTRAN, BASIC, APL, and C and many worked-out examples illustrating computational procedures. Compilable source codes for all programs are included in a floppy disk, which is packaged with the book and formatted for the IBM PC or compatible computers. For the numerical analyst, the most interesting part of the book is Chapter 11, which describes how techniques of numerical linear algebra such as QR factorizations, Householder reflections, Cholesky factorizations, and LU factorizations can be applied to least squares problems.

The book is eminently suitable as a guide for the practitioner because of its careful expository style and its stress on "hands-on" computations. The mathematical prerequisites are elementary linear algebra and a first course in statistics. Fluency in at least one programming language is assumed.

H. N.

18[11-01, 11A51, 11Y05, 11Y11].—DAVID M. BRESSOUD, *Factorization and Primality Testing*, Undergraduate Texts in Mathematics, Springer, New York, 1989, xiii + 237 pp., 24 cm. Price $45.00.

Is it possible to teach an undergraduate, beginning number theory course by focusing almost entirely on factoring and primality testing? The thought is that these topics use so much number theory that little in a standard course would be left out. This is Bressoud's premise and his book is a text for such

a course. Of course, some factorization and primality testing algorithms would be difficult to present at this level, but enough remains to make a nicely rounded book. Bressoud even gets to the elliptic curve method for factoring, minus most proofs though.

There is a definite "hands-on" flavor to the book. The algorithms presented are meant to be tried out by the students. (It is assumed that one has access to high-level software that can deal with long integers.) Actual programs are given for many algorithms, written in a kind of shorthand Pascal, that should be easily translatable into code by someone who knows programming. Some of the more advanced topics reached include the $p \pm 1$ factoring methods, the rho method, the quadratic sieve and continued fraction factoring algorithms, pseudoprimes, the $p \pm 1$ primality tests, and, as mentioned above, elliptic curve factoring.

One unfortunate omission is random compositeness testing. It would have been a simple matter for Bressoud to have developed the Solovay-Strassen (random Euler) test or the Miller-Rabin (random strong probable prime) test. The latter is just barely missed—see the comments on p. 78 and exercise 6.21. Sometimes poor advice is offered. For example, on p. 70, Bressoud seems to say that the $p - 1$ and rho methods should be tried with several random seeds, rather than pushed further with one seed. This is apt advice for elliptic curve factoring, but not for $p - 1$ or rho.

There are several typographical conventions that were glaring to my eye. One is the consistent use of $\times$ as a times sign—we consistently see expressions like $2\times k$ for $2k$ and $a\times b$ for ab. Another is the use of ∂ as a group operation and # for group exponentiation—I suppose this is to favor neither multiplicatively nor additively presented groups. Nevertheless, equations such as $x\#3 = x\partial x\partial x$ are jarring.

If you want a book delving deeply into the theory and practice of factoring and primality testing, this is not a good choice (nor does it purport to be). If you want to teach a beginning number theory course to computer-literate students and get to many interesting and powerful methods, this book is your text. Overall, the style is very friendly and inviting, and I think students who like to program will enjoy it.

C. P.

19[11-01, 11A41, 11D09, 11E25, 11R37, 11G15].—David A. Cox, *Primes of the Form x^2+ny^2: Fermat, Class Field Theory, and Complex Multiplication*, Wiley, New York, 1989, xi + 351 pp., 24 cm. Price $42.95.

Number theory, perhaps more than any other branch of mathematics, is organized around great problems. It is characterized not by the techniques used, which may come from algebra, analysis or geometry, but rather by the questions which are asked. For this reason, instead of biting off some general theory to write about, the author of a number theory textbook is often tempted to choose a tantalizing conjecture, or old riddle, as the book's unifying theme.