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.

The classical problem around which David Cox organizes his book is: Given a positive integer n, find a way of telling which primes p can be written in the form $x^2 + ny^2$ for some integers x, y. The simplest and best known case is $n = 1$, where the answer, due to Fermat, is: if and only if $p = 2$ or $p \equiv 1 \mod 4$.

The goal is the following theorem, which in some sense solves the problem: *Given n, there exists a polynomial $f_n(x)$ with integer coefficients such that a prime p can be written in the form $p = x^2 + ny^2$ if and only if $-n$ is a quadratic residue modulo p and $f_n(x) \equiv 0 \mod p$ has a solution.*

The book starts by developing the elementary methods that suffice for certain values of n: quadratic, cubic and biquadratic reciprocity; reduction of positive definite quadratic forms; and genus theory. The next part is devoted to class field theory. Using a classical approach to the subject, the author shows how the basic theorem about the existence of the polynomials $f_n(x)$ follows from the Artin Reciprocity Theorem. The final third of the book is concerned with the problem of constructing the $f_n(x)$ in the theorem for a given n; this leads to elliptic functions, complex multiplication, and properties of the j-function.

The book concludes with a discussion of the Goldwasser-Kilian-Atkin primality test using elliptic curves over finite fields and the theory of complex multiplication. There is an ample supply of exercises throughout the text.

The book is a welcome addition to the expository literature. The writing is informal, enthusiastic, and enriched with extensive historical information.

The reader should be warned, however, that few sections of the book are self-contained. For most of the central theorems either the entire proof or the hardest part of the proof is not given (but references are always supplied). For example, the basic theorems of class field theory, the results of Deuring, Gross, and Zagier on the class equation, and even cubic and biquadratic reciprocity, are all stated without proof.

The author's primary purpose is not to give proofs, but rather to motivate, to trace the threads of a fascinating story, and along the way to explain some difficult ideas of modern algebraic number theory in a down-to-earth way. In this he succeeds admirably.

The author claims that the first third of the book is suitable as a supplementary text in a beginning undergraduate number theory course. I disagree. The pace of exposition and the difficulty of exercises are likely to leave undergraduates more confused than enlightened. In his impatience to get to advanced topics, the author shortchanges the more routine matters.

For example, the first proof in the book is of the theorem that an odd prime p can be written as $x^2 + y^2$ if and only if $p \equiv 1 \mod 4$. The proof starts out by stating the two basic assertions to be proved:

Descent Step: If $p | x^2 + y^2$, $\gcd(x, y) = 1$, then p can be written as $x^2 + y^2$.

Reciprocity Step: If $p \equiv 1 \mod 4$, then $p | x^2 + y^2$, $\gcd(x, y) = 1$.

Both statements are likely to confuse a student—the first because the x and y

at the end are not the same as the x and y at the beginning, and the second because of missing quantifiers. Moreover, the proof that follows contains a gap: one needs to know that a nontrivial divisibility $p|x^2 + y^2$ implies that $p \equiv 1 \mod 4$, since otherwise (middle of p. 11) one cannot rule out the possibility that N is the product of p and a prime $q \equiv 3 \mod 4$.

This type of imprecision, while not likely to discourage a sophisticated reader, does diminish the book's value for undergraduates.

To summarize, David Cox's book is an excellent textbook and reference for people at the graduate level and above.

NEAL KOBLITZ

Department of Mathematics
University of Washington
Seattle, Washington 98195

20[11-00, 65-00].—JONATHAN BORWEIN & PETER BORWEIN, *A Dictionary of Real Numbers*, Wadsworth & Brooks/Cole Advanced Books & Software, Pacific Grove, California, 1990, viii + 424 pp., $28\frac{1}{2}$ cm. Price $69.95.

This book is quite accurately described by its title. The authors have catalogued approximately 100,000 "interesting" real numbers, indexing them lexicographically according to the first eight digits following the decimal point. Both pure mathematical constants and some constants of physics are included.

Such a listing could be quite valuable as a reference book for a mathematician, computer scientist or physicist who in the course of a calculation, either theoretical or empirical, produces some number whose identity is not known. If such a number is found in this listing, and computation to higher precision confirms its equality to the constant in the list, then one can pursue a rigorous proof with a high level of confidence. In other words, a listing of this sort could enable mathematicians to employ "experimental" techniques in their research.

To their credit, the authors give a definition in the Introduction of exactly what numbers are included in the list. It is worth briefly summarizing this definition. Their listing is based on a "standard domain" of 4,258 numbers. These numbers consist of

1. Certain simple rational numbers.
2. Rational multiplies of certain irrational and transcendental constants.
3. Square roots and cube roots of small integers and simple rational numbers.
4. Elementary functions evaluated at certain simple values.
5. Sums and differences of square roots of certain small integers.
6. Rational combinations of certain constants.
7. Euler's constant, Catalan's constant, and some constants from physics.

All other numbers in the listing are either combinations of values of elementary functions, real roots of cubic polynomials with small coefficients, or special functions evaluated at numbers in the "standard domain" defined above.