BRESSOUD, D. M., *Factorization and primality testing* (Undergraduate Texts in Mathematics, Springer-Verlag, Berlin–Heidelberg–New York 1989), pp. xiii+237, 3 540 97040 1, DM 98.

The resurgence of constructive mathematics in recent years, aided no doubt by the desk-top computer, is greatly to be welcomed. There is certainly an extra feeling that one has matters under control if one can show not only *that* it can be done, but also *how* it can be done. And when one can readily write a program to actually *do* it, even when this involves a complicated algorithm impossible even to contemplate by hand, this feeling of control is complete.

But what is *it*? For the book under review, *it* is elementary number theory, concentrating, as the title indicates, on factorization and primality testing. Throughout, the style seems leisurely, and is very readable. Alongside the standard theorem-proof format, algorithms are described both verbally and in Pascal-like pseudocode, readily transcribable into whichever high-level language the reader might want to use.

The necessary preliminary material in the book is kept to a minimum, so that the main themes of the book are soon introduced. Within these themes, the author sticks to his last, and this enables him to treat very recent techniques which, to paraphrase the beer advertisement, "other undergraduate texts cannot reach". For instance, the Multiple Polynomial Quadratic Sieve, and Lenstra's elliptic curve factoring method, are both covered in the book.

The book naturally invites comparison with other recent texts in this area having a similar flavour. Both Hans Riesel's *Prime numbers and computer methods for factorization* (Birkhäuser 1985) and Paulo Ribenboim's *The book of prime number records* (Springer 1988) are of research level, suitable also perhaps as reference rather than set texts for undergraduates. While Bressoud does not try to match the breadth of coverage of Riesel or Ribenboim, its depth, for the material chosen, is remarkably similar. Neal Koblitz's *A course in number theory and cryptography* (Springer 1987), though a Graduate Text in Mathematics, is of comparable level to Bressoud's and has a large overlap in material (pseudoprimes, elliptic curve method, RSA cryptosystems,...). Also, Bressoud's book has the definite edge over the other three texts as far as clarity of exposition is concerned.

The author is to be congratulated for his achievement in making accessible to undergraduates so much material which in most hands would certainly be restricted to postgraduate level and beyond. In doing so, he has produced a first-class text very suitable as a basis for an upper-level undergraduate course in computational number theory.

C. J. SMYTH

https://doi.org/10.1017/S0013091500005101 Published online by Cambridge University Press