BOOK REVIEWS

BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 18, Number 1, January 1988

0273-0979/88 $1.00 + $.25 per page

Prime numbers and computer methods for factorization, by Hans Riesel. Progress in Mathematics, vol. 57, Birkhäuser, Boston, Basel and Stuttgart, 1985, xvi + 464 pp., $44.95. ISBN 0-8176-3291-3

While as old as the hills, the Fundamental Theorem of Arithmetic also embodies two aspects of modern mathematics. The Fundamental Theorem states that every composite number is uniquely decomposable into primes. With such a theoretically satisfying description of the multiplicative structure of the integers as our template, we have sought out and often found analogous structure in almost every corner of mathematics. Endowing seemingly chaotic material with structure and discovering new truths as a result is unquestionably a major function of mathematics. But the Fundamental Theorem also represents another trend in mathematics, a trend that was out of favor in the middle decades of this century. Computation, algorithms, and issues of effectivity, mainstays of the last century, have enjoyed reawakened interest in this, the age of computers. The Fundamental Theorem of Arithmetic, in the active form of actually distinguishing between primes and composites and factoring the latter into primes, has played a fundamental and benchmark role in this reawakening.

It is perhaps not so widely known, but the two problems just mentioned, distinguishing primes from composites and factoring composites, are quite different. This seems paradoxical since if a factoring algorithm is applied to a prime input p, the failure of the algorithm to properly factor p should then give us the information that p is after all prime. In fact, the best known factoring algorithm of all, trial division, when exhaustively applied to every trial divisor up to $\sqrt{p}$, is also the best known primality test.

To see clearly the difference between the two problems, one need look no farther than Fermat's "little theorem": if p is prime, then $a^p \equiv a \mod p$. Since it is a simple procedure to compute the residue $a^n \bmod n$ when given a and n (this can be done in $O(\log n)$ arithmetic steps in the ring $\mathbf{Z}/n$ by the repeated squaring method), if the residue is not $a \bmod n$, then n has been revealed as composite. Yet we are no closer to factoring n.

Thus the computational side of the Fundamental Theorem of Arithmetic falls into two separate problems. The first, generally called primality testing, involves deciding if an input integer is prime or composite. Some algorithms under this general banner will prove all or most composite inputs are composite, but not say anything about prime inputs (using Fermat's little theorem