Prime Numbers: A Computational Perspective[1] *By Richard Crandall and Carl Pomerance.* Springer-Verlag, New York, 2001. $49.95. xvi+545 pp. hardcover. ISBN 0-387-94777-9.

A (rational) prime is an integer greater than 1 that has no positive integer factors other than itself and 1. The *Fundamental Theorem of Arithmetic* states that every integer greater than 1 has a factorization into powers of primes, and this factorization is unique (modulo the order of the factors). Thus, the primes are the "multiplicative building blocks" of the natural numbers. Behind these apparently simple definitions and facts lies much fascination and mystery.

For example, given a large integer N, how can we compute the prime factorization of N? The Fundamental Theorem merely states the existence and uniqueness of this factorization – it does not give any clue about how it can be computed. Since N can be represented in about $\log_2 N$ bits, a *polynomial time* algorithm is one that runs in time $O(\log N)^c$ for some constant exponent c. It is not known whether there is a polynomial-time algorithm for factoring – the best known algorithm, the *Number Field Sieve* [7], is slower than any polynomial in $\log N$, although faster than any positive power of N. Since the RSA public-key cryptosystem [9] depends for its security on the (assumed) difficulty of factoring numbers that are the product of two large primes, the search for a polynomial-time algorithm for this problem is of more than "academic" interest.

Even testing primality is nontrivial. Given a large integer p, how quickly can we decide whether or not p is prime (without necessarily finding any factors)? Fermat's little theorem is often helpful in showing that p is *not* prime, since it gives a condition that a prime must satisfy, but the converse does not hold, so we can never use Fermat's little theorem directly to prove that p *is* prime. If we are satisfied with an answer that has an arbitrarily small (but positive) probability ε of error, and we have a good source of random numbers, then there is a polynomial-time *probabilistic* algorithm for determining if p is prime. If we insist on certainty, or demand a short *proof* that p is prime, then the situation is more complicated!

The *Prime Number Theorem* states that $\pi(x)$, the number of primes $\leq x$, is approximately $\int_2^x dt/\ln t$, but what is the error in this approximation? The answer is intimately linked to the distribution of complex zeros ρ of the Riemann zeta function $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$. If, as is conjectured in the famous *Riemann Hypothesis*, these zeros all have real part $1/2$, then the error in the Prime Number theorem is $O(x^{1/2}\log x)$. Otherwise the exponent of x is strictly greater than $1/2$, and the primes behave less randomly than we expect.

Other fascinating questions and conjectures concern additive properties of primes, and the existence of primes of certain forms. For example, *Goldbach's conjecture* (actually made by Euler) is that every even integer greater than 2 can be written as a sum of two primes, e.g. $18 = 7 + 11$. Although it is highly plausible, Goldbach's conjecture has never been proved.

Mersenne primes are primes of the form $2^p - 1$, where p is a positive integer (necessarily prime). Similarly, *Fermat primes* are primes of the form $2^k + 1$, where k is a positive integer (necessarily a power of two, i.e. $k = 2^n$). It is plausible that there are infinitely many Mersenne primes, but only a finite number of Fermat primes (perhaps none after $2^{16} + 1$). Again, no one knows the truth.

The book by Crandall and Pomerance considers all these questions, and many

more. It differs from several earlier books on primes, e.g. [2, 3, 4, 5, 6], in the emphasis on algorithms, large-scale computations, and the inclusion of conjectures as well as theorems. In these respects it has some similarities to [8, 10], but the style and details of the content are quite different. There is some overlap with Cohen's book [1], but topics related to primes are covered in much more detail.

The book has nine chapters: primes, number-theoretical tools, recognizing primes and composites, primality proving, exponential factoring algorithms, subexponential factoring algorithms, elliptic curve arithmetic, the ubiquity of prime numbers, and fast algorithms for large-integer arithmetic. In many cases algorithms are described in pseudo-code. There is an Appendix giving some help in the interpretation of this pseudo-code, which is described by the authors as a "fusion of English and C". The book ends with a comprehensive bibliography and index.

Each chapter includes both "exercises" and "research problems". The exercises are of varying difficulty (not indicated in the text) and no solutions are given. In some cases they are suggestions for computational projects. The research problems are generally interesting but difficult.

The first printing of a book such as this is almost certain to contain errors, and the book under review is no exception. For example, John Pollard has pointed out some errors and inaccuracies in the discussion of his algorithms in Chapter 5. The authors have promised to post errata and updates on the Springer web site.

The book is easy to browse, and is written in a friendly style, or perhaps I should say two styles, since it is clear that the two authors have rather different styles and it is often possible to guess who wrote a particular section. However, the net result is an excellent book which is more useful and varied than either author could have produced alone.

Overall, this book by Crandall and Pomerance fills a unique niche and deserves a place on the bookshelf of anyone with more than a passing interest in prime numbers. It would provide a gold mine of information and problems for a graduate class on computational number theory.

REFERENCES

[1] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics **138**, Springer-Verlag, New York, 1993.

[2] W. Ellison and F. Ellison, *Prime Numbers*, John Wiley and Sons, New York, 1985.

[3] L.-K. Hua, *Additive Primzahltheorie*, Teubner, Leipzig, 1959.

[4] M. Huxley, *The Distribution of Prime Numbers*, Oxford University Press, London, 1972.

[5] A. E. Ingham, *The Distribution of Prime Numbers*, Cambridge Tracts in Mathematics and Mathematical Physics, No. 30, Cambridge University Press, London, 1932. Reprinted with foreword by R. C. Vaughan, Cambridge Mathematical Library series, 1990.

[6] E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, Teubner, Leipzig, 1909. Second edition (with an appendix by P. T. Bateman) reprinted by Chelsea, New York, 1953.

[7] A. Lenstra and H. Lenstra, Jr., editors, *The Development of the Number Field Sieve*, Lecture Notes in Mathematics **1554**, Springer-Verlag, New York, 1993.

[8] H. Riesel, *Prime Numbers and Computer Methods for Factorization*, second edition, Birkhäuser Boston, 1994.

[9] R. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM*, **21** (1978), pp. 120–126.

[10] S. Y. Yan, *Number Theory for Computing*, Springer-Verlag, New York, 2000.

Richard P. Brent
Oxford University