The next four chapters penetrate deeper into the theory of zeta and L-functions. Chapter 4, 'The method of contour integration', presents the classical approach to the prime number theorem based on estimates of $|\zeta(s)|$ in a region just to the left of the line $\mathrm{Re}(s) = 1$. While being technically more demanding than the approach via Tauberian theorems, this provides non-trivial error estimates. Chapter 5, 'Functional equations', proves the functional equations relating $\zeta(s)$ to $\zeta(1-s)$ and $L(x, \chi)$ to $L(1-x, \overline{\chi})$ using the Poisson summation formula. Chapter 6, 'Hadamard products', proves that the entire functions derived from $\zeta(s)$ and $L(x, \chi)$ have order 1 and so have infinitely many zeros, all in the critical strip $0 < \mathrm{Re}(s) < 1$. This is an essential prelude to Chapter 7, 'Explicit formulas', where the functions $\psi(x)$ and $\psi(x, \chi)$ governing the distribution of primes and the distribution of primes in arithmetic progressions are shown to be given by the 'explicit formulas' of Weil. These explicit formulas involve the zeros of $\zeta(s)$ and $L(s, \chi)$ in the critical strip. Here the rôle of the Riemann hypothesis becomes clear: the non-vanishing of $\zeta(s)$ to the right of the critical line $\mathrm{Re}(s) = \frac{1}{2}$ is equivalent to the estimate $\psi(x) = x + O\left(x^{1/2}(\log x)^2\right)$.

The final three chapters each deal with a single topic not usually discussed in an introduction to analytic number theory. Chapter 8, 'The Selberg class', is a brief introduction to a topic of current research: the Selberg class is a class of Dirichlet series containing the zeta and L-functions and more. Murty proves a recent theorem of Conrey and Ghosh on functions in the Selberg class; conjectures of Selberg remain elusive. Chapter 9, 'Sieve methods', deals with enumeration techniques based on sophisticated extensions of the sieve of Eratosthenes; an application to twin primes is given. Finally Chapter 10, 'p-adic methods', is an introduction to p-adic numbers, a topic dealt with more frequently in books on algebraic number theory. The main result is the p-adic interpolation of the values of the Riemann zeta-function by means of the Mazur measure and its application to congruences for the Bernoulli numbers.

This is a splendid introduction to analytic number theory, and noteworthy for its treatment of topics beyond zeta and L-functions. The writing is terse but clear. All beginning research students in number theory need familiarity with this material, and a problem-based book such as this is a fine way for them to learn the subject. It is very definitely a graduate text. While the first three chapters might form part of a fourth-year course or project at a British university, the book as a whole would only be suitable for the most enterprising undergraduate.

ROBIN CHAPMAN
School of Mathematical Sciences, University of Exeter, Exeter EX4 4QE
e-mail: *rjc@maths.ex.ac.uk*

Prime numbers: A computational perspective, by Richard Crandall and Carl Pomerance. Pp. 545. 2001. ISBN 0 387 94777 9 (Springer-Verlag).

The first chapter of the book is an introductory tour of prime number theory, ancient and modern. In it you will find the usual subjects: the distribution of the primes, leading to the prime number theorem, a introduction to exponential sums, analytic number theory, the Riemann zeta function and, inevitably, a discussion of that most famous unsolved problem of mathematics, the Riemann hypothesis. Backed by 30-odd pages of exercises and research problems, this first chapter alone should provide any interested reader with plenty of material to work on.

When one is confronted by a difficult problem and is not clear how to proceed, there is a temptation to create bigger and better examples of the objects that are causing the trouble. Such is the case with the distribution of the primes. As readers may be aware, there is a huge amount of interest in the world-wide 'Great Internet

Mersenne Prime Search', coordinated by George Woltman, which, since its inception in 1996, has had the spectacular success of delivering the largest known primes. The book has quite a lot to say about the computational aspects of this project; as well as a discussion of the Lucas-Lehmer test there is a description of the discrete Fourier transform methods for multiplying numbers having millions of digits and, in particular, the 'irrational base', weighted transform of Crandall and Fagin, as used by the 'GIMPS' project.

As the book explains, multiplying together large numbers efficiently is easy. Somewhat harder is to reverse the process: to start with a large number and determine one of its prime factors. Again, this difficult problem has attracted great interest and people are prepared to spend enormous amounts of computational power attempting to factorise numbers that have a particularly elegant representation. To take a specific example, there currently exists another world-wide cottage-industry, known as the Cunningham project, whose business it is to find prime factors of numbers of the form $b^n \pm 1$ for $b = 2, 3, \ldots, 12$ and n as large as possible.

Thus we can sum up the main theme of the book: How best to use computers to find large primes and to factorise large integers.

The second chapter deals with the fundamentals of computational number theory. The emphasis is on describing efficient algorithms for essential number-theoretic processes. Algorithms are presented in a particularly nice form of pseudo-code (which should appeal to 'C' programmers); they are easy to understand and easy to implement in one's favourite programming language.

When we arrive at Chapter 3 we are ready for some serious work—the problem of determining whether a given number is prime or composite. Searching for a set of primes that have a specified property is usually achieved in three stages. First some kind of sifting procedure eliminates from further consideration sets where one member is divisible by a small prime. Second, one applies a fast and efficient probable primality test to those sets that survive the first stage. Finally, any numbers that pass the first two stages need to be verified by a primality proof before they can be released into the mathematical community. Chapter 3 describes probable-primality testing and the various types of pseudoprime. It also includes a discussion of some recent work of Grantham on Frobenius pseudoprimes. Chapter 4 deals with the primality proofs for numbers N where there is a known factorisation of a sufficient part of $N^2 - 1$. There is also a section on the general 'APR' method based on Gauss and Jacobi sums. Factorisation methods, including a working implementation of the number field sieve, are covered by Chapters 4 and 5.

The elliptic curve method for factorisation and for primality proving is the subject of Chapter 7. The reader is introduced to elliptic curves in a friendly manner with the emphasis on implementable computer procedures. The chapter includes the development of routines for performing fast and efficient arithmetic on elliptic curves, as one would want, for example, to perform powering computations. Primality proving by the elliptic curve method requires a procedure for determining the order of an elliptic group. There is an excellent and highly readable account of the theory and a discussion of computational techniques.

On the whole, the book is well-written and the pace is leisurely. It is not necessarily a coherent account of number theory; it complements rather than competes with the classic texts such as Hardy and Wright [1] and Niven, Zuckerman and Montgomery [2]. On the other hand, it is fair to say that the book covers almost every modern development relevant to its subject area. Also there is much interesting research material collected in the extensive lists of problems at the end of each chapter.

This is a wonderful book for expert number theorists or keen amateurs who want to bring their personal computing resources to bear in the search for interesting mathematical objects related to prime number theory. The only real prerequisite is a passionate interest in prime numbers and the closely related topic of integer factorisation. Although to understand the detailed mechanism of the number field sieve, or the finer points of the elliptic curve method, one would benefit from a reasonable grounding in number theory, there are large parts of the work that should, in my opinion, appeal to any determined sixth-former. For example, the book has a delightful chapter near the end, 'The Ubiquity of Prime Numbers'.

References

1. G. H. Hardy and E. M Wright, *An introduction to the theory of numbers*, Oxford University Press, 1939.
2. I. Niven, H. S. Zuckerman and H. L. Montgomery, *An introduction to the theory of numbers*, (5th edn), John Wiley, 1991.

TONY FORBES

22 St Albans Road, Kingston upon Thames KT2 5HQ

The beginnings and evolution of algebra, by Isabella Bashmakova and Galina Smirnova, translated by Abe Shenitzer. Pp. 179. £15.95. 2000. ISBN 0 88385 329 9 (Mathematical Association of America).

This book traces the history of algebra from its beginnings in ancient Babylon to roughly the end of the nineteenth century. The Babylonian heritage described in the first chapter is known through the hundreds of thousands of clay tablets found in Mesopotamia and first deciphered in the 1930s. It is clear that the Babylonians knew how to find quite large Pythagorean triples (hundreds of years before Pythagoras) and, as early as 2000BC, how to solve linear and quadratic equations. What the authors do not tell us is why the Babylonian civilisation fell: their treatment focuses firmly on the mathematics.

The next significant step is covered in the second chapter. The ancient Greeks civilisation is the first known to have developed the idea of proof, by around 500BC. As is well known, the Greeks developed an axiomatic treatment of geometry and used geometric methods to solve algebraic equations. Eventually, however, the Greeks developed a literal symbolism, exemplified in the works of Diophantus, which are described in some detail in the third chapter.

In Europe, the fall of the ancient empires led to the 'dark ages' – a period of nearly a millennium when scholarship barely survived. The algebraic 'torch' moved further east with the rise of Islam, to the Arabian empire centred on Baghdad, where al-Khwarizmi flourished in the ninth century. Indeed, the term 'algebra' comes from the title of al-Khwarizmi's book *Al-jabr wa'l muqābalah*. The Arab scholars had translations of both Greek and Hindu works and it was this eclecticism, together with the conquest of significant parts of Europe that eventually led to the renaissance of mathematics in western Europe. The long period of history from al-Khwarizmi to Leonardo of Pisa and Luca Pacioli is dealt with in chapter four, which also covers the development of algebraic notation from literal to symbolic form that occurred during this era.

From the sixteenth century, European mathematicians began to surpass the ancients. Part of chapter five describes the well-known dispute between Tartaglia and Cardano over the solution of the cubic equations. In other sections we learn about the work of Bombelli and Viète. The remainder of the book is devoted to the modern era, beginning with the eighteenth-century struggle to find a complete proof