which the mathematically literate reader will recognise as valuable and worthwhile content. However, the text dodges the issue of what assistance needs to be given if students are to proceed from informal experience to formal, useable mathematical concepts and methods. There are no hints or comments for the student, and no indication as to what the teacher has to do for the approach to succeed. Thus potentially lovely material is presented in a methodological void.

This is illustrated by the first few pages.

(a) The first section begins by trying to get students to understand *intrinsic* properties of a network – by using the informal idea of a 'bug's eye view'.

(b) By the time we get to the third task, the student is expected 'devise a precise description of what it means for two countries [i.e. networks] to be "the same" as far as the insects are concerned'.

(c) This is immediately followed by a sermon which includes the unhelpful words: 'Some Tasks are easy and some a very difficult'. There is no way for the student (or the teacher!) to know which are which, yet the sermon continues: 'so you should not expect to find a complete answer to every one. If a Task seems mysterious, it can help to discuss it with someone else. Occasionally you may skip a Task and come back to it later, but skipping a Task in the hope of finding the answers in the text will lead you nowhere.'

(d) These words are immediately contradicted – though not enough for the text to be effective. For the very next page contains an *ex cathedra* list of definitions – including that of a *graph* (though not of *graph isomorphism*). It remains unclear how the student was expected to respond to the third task referred to in (b) (which presumed the student would formulate an abstract definition of a *graph isomorphism* without having even begun to imagine the need for an abstract definition of *graph*), or why a definition of *graph* is given, but not one of *graph isomorphism.*

I suspect the book will be widely used – not because it is a good book, but because the material is attractive and the style reflects a superficial philosophy which is currently fashionable. Anyone who would like to present this material in a way which emphasises student activity and experience will find this a useful reference: they can then make up their own minds. But if they are puzzled by what they find, it might help to know that they are not alone.

TONY GARDINER
77 Farquhar Road, Birmingham B15 2QP

Gauss and Jacobi sums, Bruce C. Berndt, Ronald J. Evans, Kenneth S. Williams. Pp. 583. £45. 1998. ISBN 0 471 12807 4 (Wiley Interscience).

This book is a sterling addition to mathematical literature. To my knowledge, no other work treats this material in such comprehensive detail. The book is of interest to workers in diverse areas of inquiry in mathematics and physics, as well as being germane to much current research. Twenty-eight research problems that arise directly from the subject matter are listed following the final chapter. Consistent care has been taken to arrange the exposition clearly, and the ordering of chapters and sequencing of ideas within them is felicitous. The book is beautifully laid out and a pleasure to read. Random sampling shows that one can easily pick up the thread of discussion on any topic *in medias res*; signal evidence of the praiseworthy clarity of the writing. The authors have succeeded in their stated aim of making the book user-friendly and of rendering 'classical theorems of Gauss, Jacobi, Eisenstein, and others accessible to beginning graduate students in mathematics and physics'.

The background required for reading the book is surprisingly modest. One needs an appreciation of undergraduate modern algebra, including finite fields, and basic material in elementary and algebraic number theory, readily found in many standard texts. Some basic complex analysis is used in Section 1.2; some p-adic analysis in Sections 1.6, 9.3 and 11.2, though alternative arguments given in Section 1.6 avoid p-adic analysis. Many applications of Gauss and Jacobi sum evaluations are investigated; not only to number theory, as might expected, but also to physics and to such areas of mathematics as graph theory and combinatorics, operator theory, coding theory, cryptography, combinatorial designs, analysis and algebra.

The preface explains that Gauss, in his *Disquisitiones Arithmeticae* of 1801, introduced the sum $g(m; k) = \sum_{n=0}^{k-1} e^{2\pi imn^2/k}$, which is now called a quadratic Gauss sum. This sum is not easy to evaluate, even in the special case where $m = 1$ and k is an odd positive integer. Gauss was easily able to show that the sum has the value $\pm\sqrt{k}$ or $\pm i\sqrt{k}$, according as k has the form $4u + 1$ or $4u + 3$, respectively, but determining that the plus sign is always correct, took him another four years to establish. Subsequently, he was able to evaluate his quadratic sum for all positive integers k. Jacobi introduced the sum named after him in a letter to Gauss, dated 8 February 1827. Dirichlet, in his study of primes in arithmetic progressions, introduced the multiplicative character χ modulo k and the sum $G(\chi) = \sum_{n=0}^{k-1} \gamma(n) e^{2\pi imn/k}$ which is now also called a Gauss sum.

The first two chapters dealing with basic material on Gauss and Jacobi sums over finite fields are fundamental to the rest of the book. In the first chapter, after establishing a certain multiplicative property of Gauss sums, Gauss's proof of the law of quadratic reciprocity is given. Then Gauss's evaluation of $g(1; k)$, based on properties of the so-called Gaussian polynomials, and Estermann's elegant evaluation of $g(1, k)$, published in 1945, are presented. Section 1.5 contains an elementary determination of $g(m; k)$, with m and k coprime and $k > 0$, based on the results of the preceding sections. This chapter typifies the lucidity of exposition found throughout.

The a uthors give chapter summaries in their preface. A shortened version of these follows to indicate the contents of the later chapters.

Chapter 3: Values of Jacobi sums over F_p of orders 3, 4, 5, 6, 7, 8, 10, 12, 16, 20, and 24 are determined explicitly. They are, used often in later parts of the book.

Chapter 4: Similar evaluations are made for Gauss sums of various orders.

Chapter 5: The work of Chapter 4 is applied to the existence or non-existence of nth power residue-difference sets for some small values of n.

Chapter 6: Properties of Jacobsthal sums are developed with applications to the distribution of quadratic residues modulo p, and to congruences for binomial coefficients modulo p.

Chapter 7: Gauss sums and cyclotomic numbers are applied to establish necessary and sufficient conditions for certain primes (especially 2 and 3) to be k-th power residues modulo a prime $p = kf + 1$, where k =1, 3, 4, 5,8, and 16.

Chapter 8: Laws of cubic and quartic (biquadratic) reciprocity we taken up along with quartic, octic, and bioctic rational reciprocity laws that have a more recent history.

Chapter 9: Congruences for binomial coefficients modulo p and the difficult problem of extending such congruences modulo p^2 are examined.

Chapter 10: Properties of generalised Jacobi sums over finite fields are developed and used to determine the number N of solutions to certain diagonal equations over finite fields, or to give upper and lower bounds for N.

Chapter 11: Stickelberger's congruence for Gauss sums and the prime ideal factorisations of Gauss and Jacobi sums are included. In the final section of this chapter, a large number of results from previous sections are applied to determine the weight distribution of certain irreducible cyclic codes.

Chapter 12: Eisenstein sums over finite fields are investigated. (According to the authors those are undeservedly neglected by textbooks.)

Chapter 13: Brewer character sums, introduced in the 1960s, are studied.

Chapter 14: Eisenstein's reciprocity law for k-th power residue symbols, where k is an odd prime, and Western's extension to prime powers k are discussed. (This extension is not covered in textbooks.) Gauss and Jacobi sums are used to give a considerably simplified version of Western's result. An extensive bibliography, in an attractive format, is provided at the end.

Every precaution is taken to help the reader navigate the daunting technicalities of the subject, Commonly, at the beginnings of chapters, notational conventions are summarised; at the head of each section the conventions are particularised. Well-designed tables detail important information. Statements of theorems, propositions, etc, are clear and complete.

A generous collection of exercises, encompassing all ranges of difficulty from the routine to those offering new results, is found at the end of each chapter. After each set of exercises, informative notes indicate the history of results established in the chapter, and discuss current research on related matters. Connective prose contains apposite remarks about the significance of a theorem about to be stated, or explicates the history and pertinent facts concerning some conjecture, while worked examples enable the reader better to appreciate the import of many results.

This definitive treatise will work equally as an instrument of instruction or as a reference source. Admirably written, it is the quintessence of scholarship.

PETER CASS

Department of Mathematics, Middlesex College, University of Western Ontario,
London, Ontario, Canada N6A 5B7

Introduction to the theory of error-correcting codes, 3rd edition, by Vera Pless. Pp. 207. £38.95. 1998. ISBN 0 471 19047 0 (Wiley).

Suppose that you intended to send a message consisting only of binary digits, for example to transmit a pattern of black and white dots. Without an error-correcting facility the received message may contain transmission errors, so that the intended message 11001110 is received as 11011101. For a very simple idea of an error-correcting code, imagine that each dot is encoded, not by a single digit, but by three digits which may be thought of as representing the vertices of a unit cube. However, only two of the vertices, those at (0,0,0) and (1,1,1) correspond to allowable codes. Each 0 of the original message is now encoded as 000 and each 1 as 111. The message sent would now be 111111000000111111111000. If it contained errors in 25% of the digits, it might arrive as 111111000100111010110001. If we group the digits in threes we detect where errors have occurred quite easily: 111 111 000 100 111 010 110 001. There are errors in the fourth, sixth, seventh and eighth blocks, since they do not contain allowable codes. Continuing with the cube-vertex analogy, we replace each incorrect code by whichever of the vertices 000 or 111 is nearest to it. The message is now automatically 'corrected' to 111 111 000 000 111 000 111 000. The sixth block has been 'corrected' the wrong way because there were two digit swaps in the block.