The Book Review Column[1]

by Frederic Green

Department of Mathematics and Computer Science
Clark University
Worcester, MA 01610
email: fgreen@clarku.edu

In this column we review two books, both mathematical, the second containing more of an emphasis on applications:

1. **Number Theory: An Introduction via the Density of Primes, Second Edition**, by Benjamin Fine and Gerhard Rosenberger. An introduction to number theory, from a predominantly analytical perspective, incorporating some of the theory underlying cryptography and primality testing. Review by Frederic Green (the second in my series on number theory; more to follow).

2. **Codes, Cryptology and Curves with Computer Algebra** by Ruud Pellikaan, Xin-Wen Wu, Stanislav Bulygin and Relinde Jurrius. Another text that introduces techniques from algebra, geometry, algorithms, and complexity, as applied to coding theory and cryptology. Review by S.V. Nagaraj.

At present I have a record number[2] of reviewers working on various titles, and expect to be including more in upcoming columns. Please let me know if you'd like to write a review; it could be among the books listed on the next page, or, if you are interested in anything not on the list, just send me a note.

[1]
[2] (for me, anyway!)

BOOKS THAT NEED REVIEWERS FOR THE SIGACT NEWS COLUMN

Algorithms

1. *Tractability: Practical approach to Hard Problems*, Edited by Bordeaux, Hamadi, Kohli
2. *Recent progress in the Boolean Domain*, Edited by Bernd Steinbach
3. *Finite Elements: Theory and Algorithms*, by Sahikumaar Ganesan and Lutz Tobiska
4. *Introduction to Property Testing*, by Oded Goldreich.
5. *Algorithmic Aspects of Machine Learning*, by Ankur Moitra.

Miscellaneous Computer Science

1. *Actual Causality*, by Joseph Y. Halpern
2. *Elements of Causal Inference: Foundations and Learning Algorithms*, by Jonas Peters, Dominik Janzing, and Bernhard Schölkopf.
3. *Elements of Parallel Computing*, by Eric Aubanel
4. *CoCo: The colorful history of Tandy's Underdog Computer* by Boisy Pitre and Bill Loguidice
5. *Introduction to Reversible Computing*, by Kalyan S. Perumalla
6. *A Short Course in Computational Geometry and Topology*, by Herbert Edelsbrunner
7. *Partially Observed Markov Decision Processes,* by Vikram Krishnamurthy
8. *Statistical Modeling and Machine Learning for Molecular Biology*, by Alan Moses
9. *The Problem With Software: Why Smart Engineers Write Bad Code,* by Adam Barr.
10. *Language, Cognition, and Computational Models,* Theirry Poibeau and Aline Villavicencio, eds.

Computability, Complexity, Logic

1. *The Foundations of Computability Theory,* by Borut Robič
2. *Applied Logic for Computer Scientists: Computational Deduction and Formal Proofs*, by Mauricio Ayala-Rincón and Flávio L.C. de Moura.
3. *Descriptive Complexity, Canonisation, and Definable Graph Structure Theory*, by Martin Grohe.

Cryptography and Security

1. *Cryptography in Constant Parallel Time,* by Benny Appelbaum
2. *Secure Multiparty Computation and Secret Sharing*, Ronald Cramer, Ivan Bjerre Damgård, and Jesper Buus Nielsen
3. *A Cryptography Primer: Secrets and Promises*, by Philip N. Klein

Combinatorics and Graph Theory

1. *Finite Geometry and Combinatorial Applications*, by Simeon Ball
2. *Introduction to Random Graphs*, by Alan Frieze and Michał Karoński
3. *Erdős –Ko–Rado Theorems: Algebraic Approaches*, by Christopher Godsil and Karen Meagher
4. *Combinatorics, Words and Symbolic Dynamics,* Edited by Valérie Berthé and Michel Rigo

Miscellaneous Mathematics

1. *Introduction to Probability*, by David F. Anderson, Timo Seppäläinen, and Benedek Valkó.

Review of[3]
Number Theory: An Introduction via the Density of Primes, second edition
by Benjamin Fine and Gerhard Rosenberger
Springer, 2016
413 pages, Hardcover or softcover, $79.

Review by
Frederic Green (fgreen@clarku.edu)
Department of Mathematics and Computer Science
Clark University, Worcester, MA

There are probably at least as many different approaches to number theory as there are books written about it. Some broad distinctions include those taking an historical versus (say) a purely modern approach, with many gradations in between, or those that are algebraically oriented (e.g., with an emphasis on reciprocity laws, or questions that relate to algebraic geometry), or still others that are more analytic. The book under review is definitely in the latter category. The "message" of the book is in the title, as primes and their density are the principle concern. In accordance with that theme, a highlight of the book is a complete proof of the prime number theorem. However, the theme and its variations are taken as springboards to other important fields, including aspects of algebraic number theory, as well as applications, such as primality testing and cryptography.

1 Summary of Contents

There aren't many chapters, but most of them are fairly long and chapters 3 and 4 are practically books in themselves.

1. Chapter 1: Introduction and Historical Remarks. This is a short overview, largely historical and motivational, although it should be noted that historical remarks also appear (in suitably augmented detail) at many appropriate points in the course of later chapters.

2. Chapter 2: Basic Number Theory. This is an introduction to elementary number theory, beginning with standard concepts such as divisibility, primes, and composites. The division and Euclidean algorithms are given, as is a proof of the fundamental theorem of arithmetic. Congruence leads to results such as the Chinese Remainder Theorem as well as algebraic concepts such as groups, rings, and fields. These are studied in sufficient depth for introducing other basics such as Lagrange's Theorem, Fermat's little theorem, and primitive roots. We see polynomial congruences, quadratic residues, and quadratic reciprocity, proved via a geometric method of Eisenstein (one of the numerous proofs of this famous theorem[4]).

3. Chapter 3: The Infinitude of Primes. This is the first chapter that clearly distinguishes this text from others. Section 3.1 presents a great variety of proofs that there are infinitely many primes. Of course we begin with Euclid. But other arguments include elementary techniques using factorials or the Euler ϕ-function; analytic methods based on the divergence of sums like $\sum_{p\ prime} \frac{1}{p}$, including one based on

[3] ©2019, Frederic Green
[4] N.B. my reviews in SIGACT News **49**(1) (2018), pp. 20–28

the Riemann Zeta Function and the Euler product expansion thereof, which methods ultimately point in the direction of the prime number theorem. Fermat and Mersenne numbers lead to further proofs, which in turn indirectly point in the direction of Dirichlet's Theorem. The Fibonacci numbers offer an entertaining digression, and also yield two slick proofs of the infinitude of primes. We next look at some easy cases of Dirichlet's Theorem, e.g., there are an infinite number of primes in the progression $\{4n + 3\}$, which follow from Euclid-type arguments and very basic properties of congruences. In order to get to Dirchlet's Theorem in general, Section 3.2 takes a detour through the Fermat sum of two squares theorem, including the number of such representations of an integer (assuming it has one). Dirichlet characters and the Dirichlet L-function emerge naturally in this context. An exposition of the modular group yields another proof of the sum of two squares theorem. An elementary proof of Lagrange's sum of four square theorem is presented, and Section 3.2 concludes with a proof of the infinitude of primes via continued fractions. The chapter culminates in a proof of Dirichlet's theorem on primes in arithmetic progression. The hard part (that $L(1, \chi) \neq 0$ when χ is a non-principle real Dirichlet character) is proved via a self-contained "elementary" analytical (not making use of *complex* analysis, although still not easy) proof. The chapter concludes with some discussions of the twin prime conjecture, Bertrand's Theorem (there exists a prime between x and $2x$, proved in the next chapter), and various arithmetic functions including a proof of the Möbius inversion formula.

4. Chapter 4: The Prime Number Theorem ("PNT"). The chapter begins by setting the stage with some historical remarks and stating PNT, that the prime-counting function $\pi(x)$ approaches $x/\ln x$ asymptotically. It then presents Chebyshev's estimate, which states that $\pi(x)$ is of the same order of magnitude as $x/\ln x$, using a relatively simple proof based on inequalities involving the binomial coefficients. One then obtains some corollaries, e.g., Bertrand's Theorem, as promised in the previous chapter. As a prelude to the proof of PNT, necessary properties of Chebyshev's functions (θ and ψ) are proved, e.g., the equivalence of $\psi(x) \sim x$ and PNT. A proof is also given of Chebyshev's theorem that if $\pi(x)/(x/\ln x)$ has a limit, it must equal 1. In his day it seemed that Chebyshev was very close to a proof of PNT, but it was decades before the famous complex-analysis-based proof was discovered independently by Hadamard and de la Vallée Poussin in 1896. Further preparation for PNT is provided by a brief but very clear introduction, without proofs, to the necessary complex analysis (e.g., contour integration, the Cauchy integral formula, and analytic continuation), and properties of the zeta function. Most importantly, it is proved that there are no zeroes of $\zeta(s)$ along the line $\Re s = 1$, an assertion that is equivalent to PNT, as is proved in the following section. That section also contains the highlight of the chapter (and one of the highlights of the book), an elegant complex-analytical proof of PNT via a technique of Newman from 1980, which greatly simplifies the proofs of Hadamard and de la Vallée Poussin. The chapter closes with three sections. The first gives an overview, mostly without proofs, of the so-called "elementary" (non-complex-analytic, but still complicated!) proof of PNT due to Erdős and Selberg, which greatly extended the work initiated about 100 years earlier by Chebyshev. The second reviews the state of our knowledge (and ignorance) of the values of $\zeta(n)$ for $n \in \mathbb{N}$. Euler determined $\zeta(2k)$ for all $k \in \mathbb{N}$ (the formula involving π and the Bernoulli numbers is proved in this section), but it is not even known now if $\zeta(3)$ is transcendental (Apéry's Theorem, as recent as 1979, says it is irrational). This is connected to the idea of "multiple zeta values," multi-argument generalizations of the zeta function that yield insights into the values of the original zeta function, especially for odd arguments (this material is new to this edition). The final section discusses various extensions of PNT, including famous open problems such as the Riemann Hypothesis and its generalizations.

5. Chapter 5: Primality Testing – An Overview. The chapter begins with basic sieving methods such as the Sieve of Eratosthenes and Legendre's formula that quantifies it. This leads naturally to Brun's remarkable theorem relating to the twin primes conjecture, namely that the sum over primes p of $\frac{1}{p} + \frac{1}{p+2}$ converges. The chapter moves on to primality testing proper, going over elementary ideas such as the Fermat Probable Prime Test and the Lucas Test, but quickly getting into the notion of *efficient* algorithms. These begin with the breakthrough AKS algorithm, the one known *deterministic* test that runs in polynomial time. The proof that the algorithm works (modulo some material relating to cyclotomic fields, which is outside the scope of the book) is relegated to a later section[5]. We next encounter probabilistic algorithms, based on the Fermat test, such as the Miller-Rabin and Solovay-Strassen tests. Results necessary to establish correctness of these algorithms are proved. There is a nice treatment of the elegant Lucas-Lehmer test for Mersenne primes, indispensable in obtaining record primes (as these are generally Mersenne[6]). Other methods discussed include elliptic curve-based tests (based on a quick exposition on elliptic curves!), in particular a concrete and accessible presentation of the Goldwasser-Killian prime number certification algorithm. Applications of these methods are given in sections on cryptography, which explain the relationship between primes and (most) cryptographic schemes. These sections also include introductions to public key cryptography based on RSA and elliptic curves. The chapter concludes with an exposition of the mathematics underlying the AKS algorithm.

6. Chapter 6: Algebraic Number Theory. This begins with the basics of unique factorization domains. This includes integral domains, the Euclidean algorithm, Euclid's Lemma, and Euclidean domains, as exemplified by the Gaussian integers. The development continues with principle ideal domains (PID's), and it is proved, via the ascending chain condition, that every Euclidean domain is a PID. Kronecker's Theorem is a natural segue to algebraic number fields. Field extensions are initially defined in general terms, but then specialized to algebraic extensions. The notions of discriminant, norm, and trace are introduced preparatory to a study of rings of algebraic integers, such as the properties of primes in such rings (e.g., factorization into primes, and that they are infinite in number). Quadratic fields and rings of quadratic integers are introduced as well. Salient properties of fundamental units (e.g., their infinitude in real quadratic fields), in which Pell's equation plays an essential role, are proved, and then generalized to the Dirichlet Unit Theorem in a later section. The transcendence of e and π over the rationals is proved. The chapter concludes with an introduction to ideal theory, with proofs of unique factorization into prime ideals in rings of algebraic integers, a brief introduction to ideal class groups, and finiteness of the class number, which follows from material earlier in the chapter on the geometry of numbers.

7. Chapter 7: The Fields $\mathbb{Q}_p$ of p-adic Numbers: Hensel's Lemma. This chapter begins with a self-contained exposition of the construction of the real numbers via Cauchy completions. By applying the non-archimedean p-adic valuation, these ideas are then used to construct the (very different) p-adic fields $\mathbb{Q}_p$, as well as the p-adic integers $\mathbb{Z}_p$. It is proved that $\mathbb{Z}_p$ is a PID, and hence a unique factorization domain. The chapter concentrates on working out the general properties of p-adic numbers. Thus, for example, a proof is given of Ostrowski's theorem (that any "absolute value" on $\mathbb{Q}$ is either trivial, the standard Euclidean absolute value, or one of the p-adic norms). Near the end of the

[5] See also the book of Rempe-Gillen and Waldecker, devoted entirely to the AKS algorithm, reviewed in this column, SIGACT News **47**(2), (2016), pp. 6–9.

[6] As this review was in preparation, news broke that the 51^{st} Mersenne prime, $2^{282,589,933} - 1$, had been discovered; see `https://www.mersenne.org/primes/?press=M82589933`.

chapter is a treatment of Hensel's Lemma, the p-adic analog of Newton's method, which provides an algorithm for finding p-adic solutions of polynomial equations over $\mathbb{Z}_p$. This section concludes with an application that establishes the equivalence of square roots in $\mathbb{Z}_p$ and quadratic residuacity.

2 Opinion

For starters, who is the book for? Like any serious math text, it is definitely not one you can read without active pencil and paper (or chalk and blackboard). However, for all proofs that I followed with some degree of care, there was always more than enough implicit detail to fill in the gaps. Each chapter also concludes with a set of exercises, of varying difficulty. Thus to get anything out of this book one needs a substantial amount of mathematical maturity, say at the level of a third or fourth-year undergraduate. No graduate student should have any problem with it. Thus it would serve well as a textbook at either the advanced undergraduate or beginning graduate level. I found it eminently suited to self-study.

In writing this book as they did, the authors have made many choices with admirable pedagogical consequences. For example, by approaching the infinitude of primes from so many different angles, we encounter a diverse set of different ideas that are important to number theory (Fibonacci numbers, the Riemann Zeta function, continued fractions, Dirichlet characters and L-functions, the Möbius inversion, etc.). While it is remarkable how many distinct proofs of the infinitude of primes exist, what is more remarkable is that these distinct proof methods are *useful*! We see this in generalizations such as Dirichlet's Theorem. Although Chapter 3 is nominally about the infinitude of primes, it leads to more general results, and in subsequent chapters there are many "teachable moments" where the authors point out yet other proofs. Such proofs crop up in unexpected places; where one might have expected an *application* of the infinitude of primes, often a new proof is lurking.

Naturally, Chapter 4 gets to the very heart of what the book is about. It is clearly presented and well explained, providing ample motivation for the approach that is taken. For example, it is a very nice touch to include historically intermediate results, such as the results of Chebyshev that seemed at one time to be very close to a proof of PNT (and indeed, a century later, led to Erdős and Selberg's "elementary" proof), rather than launching immediately into a polished proof without giving any conception of the twists and turns that led to it over the span of many years.

The later chapters may initially seem out of place, but as one reads through them, it's easy to see how well they fit in. For example, many tests for primality rely on density properties, e.g., probabilistic tests are dependent on the distribution of pseudoprimes or Carmichael Numbers. The chapter on algebraic number theory gives a very nice, succinct introduction to the field, but again, primality is the focus: the emphasis is ultimately on prime factorization of ideals. And along the way the text takes a number of opportunities to explain central algebraic concepts, such as rings, fields, cosets, quotients, etc. The material on extension fields provides a good foundation for Galois Theory. Chapter 7, on p-adic numbers, is a new chapter for this edition, and it is a very apt addition, firstly because p-adic analysis is an essential component of modern number theory, secondly because it is another way to complete the rational numbers which depends crucially on primes, and finally because it directly deals with notions of density (an ordered normed field is a dense subset of its (unique) completion). It might be outside the scope of such a text to delve into substantial applications of p-adic analysis (e.g., the Hasse-Minkowski Theorem), as they are pretty deep, but the chapter does a very fine job of gently guiding the reader through an introduction to *and* appreciation of the subject.

It is very rare for a book not to have any flaws, and this book is no exception. For example, as editor of these columns, I am these days inordinately mindful of lapses in grammar, usage, or punctuation, that I can't avoid noticing things which many other readers might not. For example, on page 108, we learn "Wieferich proved Waring's problem about cubes that is every number can be written as a sum of nine cubes." Without commas after "cubes" and "is" this is almost grammatical, and makes almost perfect sense. But it is nevertheless awkard. For other examples, on page 111: one should not say "*a* infinite simple continued fraction…," but "*an* infinite…." A few lines later, we read "that is the limit of convergent exists," rather than "that is**,** the limit of *the* convergent exists." There are also a fair number of typos and incorrect references to theorem numbers and, on occasion, section numbers. There is little doubt that many of these are artifacts of the transition from first to second edition. While these are all minor quibbles, they are numerous enough to be worthy of mention. I point out these issues not to criticize the book's readability (as it is, in other respects, eminently readable), but rather to indicate how that readability may be improved.

That being said, this book grew on me as I read through it. And I learned a lot from it! Among its many attractive features is that it strives successfully to be reasonably self-contained, relying on very few prerequisites (beyond the mathematical maturity as mentioned above). While it assumes some familiarity with basic algebraic concepts (linear algebra, group theory), the background it assumes is minimal (*not* assuming, for example, much more than a passing familiarity with finite fields or Galois Theory). Starting with that minimal background, it gets to some very important results. But most of all, framing the subject in terms of the density of primes provides the reader with a valuable perspective, and easily understood ideas which provide a foundation for deep results. It is an aspect of number theory that continues to drive the field, and hence it is quite effective in motivating and introducing the reader not only to the analytic theory, but also to the subject more broadly conceived. This introduction via the density of primes is very well done indeed.

Review of[7]
Codes, Cryptology and Curves with Computer Algebra
Ruud Pellikaan, Xin-Wen Wu, Stanislav Bulygin and Relinde Jurrius
Cambridge University Press, 2017
Paperback, ISBN 9780521520362, 606 pages, $64.99

Review by
S.V.Nagaraj (svnagaraj@acm.org)
VIT, Chennai Campus, India

1 Introduction

Codes, cryptology and curves are widely used today for secure as well as reliable communication. This book aims to introduce these topics to students of computer science, mathematics and physics at the masters level. It also looks at the application of computer algebra for solving related problems. It consists of twelve chapters contributed by four authors and published by Cambridge University Press. The book is also available in hardback and e-book formats, the price/ISBN being US$160/9780521817110, and US$52/9781108547826, respectively.

2 Summary

The book consists of twelve chapters, each authored by a subset of the four authors of the book. Three quarters of the book, the first eight chapters, discusses coding as related to error-correction.

The first chapter introduces error-correcting codes. Richard Hamming had a major role in bringing in the mathematical theory of error-correcting codes. In early days, it was not anticipated that these codes would play a crucial role in communication. Even Hamming could not have visualized a field that would encompass algebraic geometry, combinatorics, Galois theory, group theory, linear algebra, and more. The main purpose of error-correcting codes is to transmit information over a noisy channel with zero loss. The chapter introduces block codes, linear codes, parity checks, and the dual of a code. Other topics include decoding, error probability, and equivalent codes.

The second chapter focuses on code constructions and bounds on codes. The mechanisms to derive new codes from old ones are considered. The chapter also studies ways of computing bounds on how many such new codes can be constructed. These include the Singleton bound, the Griesmer bound, the Plotkin bound, the Hamming bound, the bounds due to Gilbert and Varshamov, and asymptotic bounds.

The third chapter is on weight enumeration. It reviews methods for enumerating the weight spectrum of a code. Other topics include the extended weight enumerator, the generalized weight enumerator, and the role of the weight enumerator in the determination of the probability of the undetected error and the probability of decoding error.

[7]

The fourth chapter discusses cyclic codes, in which any cyclic permutation of elements in a codeword generates another codeword. The chapter concentrates on the structure of finite fields since it is essential for a proper understanding of cyclic codes. Zeroes, bounds on the minimum distance, the BCH (Bose-Chaudhuri-Hocquenghem) bound and improvements to it, locator polynomials, and ways of decoding cyclic codes are other topics described in this chapter.

The fifth chapter studies polynomial codes whose codewords are realized as polynomials with the code elements as coefficients. Here we find information about Reed-Solomon codes and their generalizations. The notions of Galois invariant codes, subfield subcodes and trace codes are highlighted. Other themes include families of polynomial codes and Reed-Muller codes.

The sixth chapter considers decoding by means of algebraic algorithms such as the Berlekamp-Massey algorithm, and the Euclid-Sugiyama algorithm. Decoding by error-correcting pairs and list decoding by Sudan's algorithm are other topics in this chapter. List decoding of Reed-Solomon codes and Reed-Muller codes are also discussed.

The seventh chapter looks at the computational complexity of decoding. Hard problems related to the theme of the book are focused. Difficult problems in coding theory are studied and it is shown that minimum distance decoding is NP-hard. The decision problem of decoding linear codes is shown to be NP-complete. An interesting problem is deciding whether decoding up to half the minimum distance is hard. It is shown that finding the minimum distance and decoding up to half the minimum distance are closely related problems.

The eighth chapter analyzes codes and related structures. It associates codes as mathematical objects to a number of other objects such as graphs, matroids, geometric lattices, and polynomials. We also find the connection between codes and finite geometry as well as combinatorics.

The ninth chapter provides a short introduction to cryptology, and in that way introduces content related to the second word in the title of the book. Here the goal is to prevent unauthorized access to information. Topics studied include symmetric encryption schemes (such as DES, Triple DES, and AES) and asymmetric encryption schemes (such as those based on RSA and the discrete logarithm problem), public key cryptography, other asymmetric cryptosystems such as those based on multivariate cryptography, secret sharing (such as Shamir's secret sharing scheme), encryption schemes from error-correcting codes (such as the McEliece encryption scheme, Niederreiter's encryption scheme), authentication codes, block ciphers, stream ciphers, orthogonal arrays and codes, and linear feedback shift registers.

The tenth chapter discusses the application of Gröbner bases to coding and cryptology. Elements of codewords may be viewed as coefficients of polynomials. This prompts the use of Gröbner bases, in analyzing both codes in general and cryptographic systems in particular. A Gröbner basis is a transformation of a system of polynomials that has utilitarian computational properties. Topics covered in this chapter include the solution of polynomial systems, decoding codes using Gröbner bases, and algebraic cryptanalysis.

The eleventh chapter, by Pellikaan, focuses on codes on curves. This chapter ushers in the third phrase in the title of the book, i.e., curves. A code may be viewed as a system of polynomials, so it is natural to think of the polynomials as curves and to analyze their intersections and zeroes. Thus the chapter looks at the algebraic geometry of varieties and their functions. Algebraic curves, codes from algebraic curves,

order functions, and evaluation codes are examined. The theory of algebraic curves is looked at broadly and elaboration is done for plane curves. Bézout's theorem for plane curves gives a method to derive the parameters of codes on these curves. A major result of relevance to coding is the Riemann-Roch theorem. The notions of good algebraic geometry codes and asymptotically good sequences of codes are briefly discussed.

The twelfth and last chapter of the book is on coding and cryptology from a computer algebra perspective. It reviews four computer algebra packages: Singular, Magma, GAP, and Sage. It provides examples related to error-correcting codes, cryptography, and Gröbner bases with these packages. This is done mostly by working on some of the examples furnished in the previous chapters.

3 Opinion

The origin of this book was a handwritten manuscript circa 1990 due to one of its authors (Pellikaan). The aim at the time was a book on algebraic geometry codes, with emphasis on algebraic geometry and its applications to error-correcting codes and cryptography. As time passed, the other authors joined the effort in publishing this book which brought it to its current state and title. The word *coding* is ordinarily associated with secure communication. However, in many fields such as electronics and computer science, it is also related to dealing effectively with noise and errors during information transmission and retrieval. In this book, the reader will find a unified treatment of this unusual combination (secure communication as well as reliable communication). Formulating beneficial and utilitarian codes for these two applications requires a strong mathematical basis. Practical applications of apparently abstract concepts which were long savored by pure mathematicians alone have been slowly emerging, and are presented here.

This book is intended for students studying computer science, mathematics and physics, at the masters level. The topics discussed in the book will certainly be of interest to these students. Needless to say, codes, cryptology, and curves have enormous practical significance nowadays. The book includes many algorithms, definitions, examples, exercises, notes (at the end of chapters), proofs, propositions, remarks, references to the literature (an astonishing 364 in total), and theorems. The book will surely be useful for pedagogy due to the inclusion of numerous exercises in every chapter and also due to the emphasis on computer algebra. It will also be helpful for self-study and exploration. This introductory book endeavors to explain the theory underlying error-correcting codes and cryptography.

The authors aim to strike a balance between theory and practice. While they largely succeed in that goal, I feel the coverage of cryptology could have been more extensive. Only one chapter in the book deals exclusively with cryptology. Similarly, computer algebra examples might have been interspersed with every chapter, rather than confined merely to the last chapter, which discusses it for implementing the themes in the book. The authors could also have included some challenging open problems to stimulate young minds. Nevertheless, many important topics are covered in this book which looks at the practical as well as theoretical aspects of protecting digital data that is at rest or is in motion. The mathematical rigor emphasized needs to be appreciated by the student, even though some may find it terse and abstract. The presence of exercises should make it useful as a textbook, although it could also serve as a reference work. This book provides a fine exposition of the topics to those students who are novices to the field. At the same time it will also be of interest to readers who are already familiar with some of the concepts discussed in the book. It provides a valuable schematic summary and consolidated overview of the field.