The Book Review Column[1]
by Frederic Green

Department of Mathematics and Computer Science
Clark University
Worcester, MA 02465
email: fgreen@clarku.edu

Four books are reviewed in this issue, in the following three reviews:

1. **The Art of Computer Programming, Fascicle 6: "Satisfiability,"** by Donald E. Knuth. Another installment in Knuth's monumental work. Review by John Rogers.

2. **Real-World Algorithms: A Beginner's Guide**, by Panos Louridas. A reader-friendly introduction to algorithms. Review by Ramon de Vera Jr.

3. **Quadratic Residues and Non-Residues**, by Steve Wright, and **The Quadratic Reciprocity Law** by Oswald Baumgart, translated by Franz Lemmermeyer. Two books about a topic of great importance in number theory. Joint review by Frederic Green.

As you can see, I've been reading about number theory recently, and I hope the review in this column is the first in a series. I welcome any interested readers to join in this theme, or to create others! The books listed on the subsequent page are available for review. Please send me an email if you're interested in any of them, or feel free to suggest titles not included on the list.

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. *Algorithms and Models for Network Data and Link Analysis,* by François Fouss, Marco Saerens, and Masashi Shimbo
4. *Finite Elements: Theory and Algorithms*, by Sahikumaar Ganesan and Lutz Tobiska
5. *Introduction to Property Testing*, by Oded Goldreich.

Programming Languages

1. *Practical Foundations for Programming Languages,* by Robert Harper

Miscellaneous Computer Science

1. *Elements of Parallel Computing*, by Eric Aubanel
2. *CoCo: The colorful history of Tandy's Underdog Computer* by Boisy Pitre and Bill Loguidice
3. *Introduction to Reversible Computing*, by Kalyan S. Perumalla
4. *A Short Course in Computational Geometry and Topology*, by Herbert Edelsbrunner
5. *Actual Causality*, by Joseph Y. Halpern
6. *Partially Observed Markov Decision Processes,* by Vikram Krishnamurthy
7. *The Power of Networks*, by Christopher G. Brinton and Mung Chiang
8. *Statistical Modeling and Machine Learning for Molecular Biology*, by Alan Moses
9. *Market Design: A Linear Programming Approach to Auctions and Matching,* by Martin Bichler.

Computability, Complexity, Logic

1. *The Foundations of Computability Theory,* by Borut Robič
2. *Models of Computation*, by Roberto Bruni and Ugo Montanari
3. *Proof Analysis: A Contribution to Hilbert's Last Problem* by Negri and Von Plato.
4. *Applied Logic for Computer Scientists: Computational Deduction and Formal Proofs*, by Mauricio Ayala-Rincón and Flávio L.C. de Moura.
5. *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. *Codes, Cryptography and Curves with Computer Algebra*, Ruud Pellikaan, Xin-Wen Wu, Stanislav Bulygin, and Relinde Jurrius
4. *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 and History

1. *Professor Stewart's Casebook of Mathematical Mysteries* by Ian Stewart

Review[2] of
The Art of Computer Programming
Fascicle 6 "Satisfiability"
by Donald E. Knuth
Pearson Education (Addison-Wesley), 2015
318 pages, Softcover

Review by
John D. Rogers (jrogers@depaul.edu)
School of Computing, DePaul University

1 Introduction

I entered the field of Computer Science as an undergraduate because I very much enjoyed programming. Of course, there is far more to the discipline than that and, as I studied, I found myself pursuing more esoteric topics, landing for a quite a while in the land of computational complexity theory. But programming was, and remains, my first love. And that's why, once again, I find myself reading and, at times, wrestling with yet another of Don Knuth's TAOCP fascicles.

As I have written before in this column, Knuth is able to combine a more theoretical topic, in this case the satisfiability problem, with practical approaches to solving it, approaches that encourage the reader to write some code. It's this mix of the theoretical and the practical that I, and I believe many others, find engaging.

As we all know, the satisfiability problem (SAT) is NP-complete and is considered the ur-problem of the theory. According to Bill Gasarch's survey, to which Knuth refers in a footnote on page 1, most feel we are a long way from showing whether $\mathbf{P} \neq \mathbf{NP}$. Despite that, many have realized that we can still attack large classes of SAT problems, classes coming from many practical applications, with techniques that work reasonably efficiently.

Fascicle 6 is Knuth's contribution to this and is the next in a series of paperback publications that together will form Volume 4 of "The Art of Computer Programming" (TAOCP). The volume will appear as a trilogy, with Volume 4A already in hardcover. This fascicle will be the middle third of Volume 4B.

2 Summary

To provide some context of where the work stands, here are the fascicles published to date:

- Fascicle 0, Introduction to Combinatorial Algorithms and Boolean Functions (2008)
- Fascicle 1, Bitwise Tricks and Techniques; Binary Decision Diagrams (2009)
- Fascicle 2, Generating All Tuples and Permutations (2005)
- Fascicle 3, Generating All Combinations and Partitions (2005)
- Fascicle 4, Generating All Trees; History of Combinatorial Generation (2006)

- Prefascicle 5A, Mathematical Preliminaries Redux (online beta version 2017)
- Fascicle 6, Satisfiability (2015)

There was also a Fascicle 1 for the already published Volume 1, which provided an updated version of Knuth's MMIX machine language.

To put this in the context of the larger work: Fascicle 6 contains the first published version of sub-sub-section 7.2.2.2 and is titled "Satisfiability." The previous sub-sub-section, 7.2.2.1, is "Dancing Links." These, so far, form sub-section 7.2.2, "Basic Backtrack," which, in turn, follows 7.2.1, "Generating basic combinatorial patterns." Section 7.2 is "Generating All Possibilities" and is found in Chapter 7, "Combinatorial Searching."

As Knuth himself writes, TAOCP does not allow for units indexed by five digits so he simply lists them under 7.2.2.2. Here is the table of contents as it appears in this fascicle:

These are followed by an index of the theorems and algorithms and by a book index and glossary. There is no bibliography as in-text references provide the necessary information.

After a brief introduction, Knuth provides a list of examples indicating the broad applicability of this problem.

- A simple example: Find an 8-bit sequence not containing three equally spaced 0s nor three equally spaced 1s.
- Exact covering
- Graph coloring
- Factoring
- Fault testing
- Learning a Boolean function
- Bounded model checking
- Mutual exclusion
- Digital tomography

I especially enjoyed the connections to forums with broader appeal, such as Martin Gardner's example of a planar graph requiring five colors, published shortly before the Four-Color Theorem appeared. Obviously, this *McGregor graph* does not require five colors and an exercise leads to a way to use satisfiability to find a four-coloring that minimizes the use of one color.

A series of algorithms follows. The first algorithm is Algorithm A, a somewhat convoluted backtracking algorithm expressed in Knuth's concise style. In fact, the algorithms presented here are more difficult to follow than those, say, published earlier on enumerating combinatorial objects. As was true for those, the steps do not leap quickly off the page into code. Knuth is, rightfully, striving for concise presentations in order to emphasize the high-level strategies being employed. One can certainly implement his satisfiability algorithms (and he certainly intends that) but most will require a careful investment of time understanding the steps.

Because this exposition is algorithm-driven, I have listed here the algorithms that Knuth describes and explains:

1. Algorithm A: simple backtracking (p. 28)
2. Algorithm B: backtracking with watch lists (p. 31)
3. Algorithm D: cyclic DPLL [Davis–Putnam–Logemann–Loveland] (p. 33)
4. Algorithm L: DPLL with lookahead (p. 38)
5. Algorithm X: lookahead for Algorithm L (p. 44)
6. Algorithm Y: double lookahead for Algorithm X (p. 46)
7. Algorithm I: clause learning (p. 61)
8. Algorithm C: conflict driven clause learning [CDCL] (p. 68)
9. Algorithm P: random walk (p. 77)
10. Algorithm W: walk SAT (p. 79)

11. Algorithm M: local resampling (p. 83)

12. Algorithm S: survey propagation (p. 93)

To a good approximation, they appear in order of increasing complexity and strength. It is not a stretch to say that one could develop a competition-level SAT solver with the help of the material in this book.

One should note, and Knuth does, that these are all sequential algorithms. He mentions in passing the use of parallelism and refers to a "cube and conquer" approach but does not present it.

Implementing these algorithms is, as I wrote above, challenging but once done one would like to test the result. Knuth provides 100 test cases, available for download, taken from a variety of areas. There are both satisfiable and unsatisfiable instances of SAT containing anywhere from hundreds to hundreds of thousands of variables and clauses. He also provides empirical results, expressed in terms of references to memory, for his implementations of Algorithms L and C.

Knuth's usual history presentation comes next. This is brief but he manages to reach back to Charles Dodgson and then forward quickly to the numerous developments during the past three decades, touching on Cook's discovery of the fundamental importance of satisfiability to complexity theory.

Taking up the second half of the book is the customary extensive list of exercises, 526 in all, followed by solutions, when available. These contribute greatly to understanding and working through the material and would serve for anything from a weekly homework to a long-term research project.

As Knuth concludes, he writes that there is much being done and much to do. His book serves as an excellent and thorough introduction to the work, especially for people hoping to jump into the fray.

3 Opinion

The book is written to be read in the order given. It's fairly short (133 pages) so this kind of development works well. It is short enough to be used as a text for a semester long course, although it will be a challenging semester! The US $29.99 list price ($23.99 on Kindle) makes it easy on the student budget.

One can imagine presenting the first six algorithms (A, B, D, L, X, and Y) as part of a course on combinatorial algorithms, or even the first two in an introductory algorithms course. With the mention and use of the Lovász Local Lemma, Algorithm M would fit into a combinatorics course.

It can also serve as a good introduction to SAT-solving, especially for those more interested in building software tools. As with most of his work, Knuth's intention is that readers will indeed try to code these algorithms.

Finally, and as I have written before, this book is science writing for scientists, especially computer scientists. It fills the gap between research papers and textbook pedagogy. A careful reader will find enough explanation and references to go as deeply as they wish into the subject.

One last note: Volume 4B in its entirety may not appear for a while. Fascicle 5A, which covers only mathematical preliminaries to this work, just appeared this past July. In fact, Knuth labeled it a "pre-fascicle." It does not include the sections on "Dancing Links" nor the more general material on backtracking. For the time being, Fascicle 6 is the only part of 4B in its almost final form.

Review of[3]
Real-World Algorithms: A Beginner's Guide
by Panos Louridas
MIT Press, 2017
500 pages, Hardcover, $42.85

Review by
Ramon de Vera Jr. (rdevera@acm.org)
Product Engineering Software Development Group
Micron Technology Inc.

1 Overview

According to the author, "the book was written to serve as a first encounter with algorithms." The book tries to provide an understanding of algorithms that can be commonly encountered by people in different disciplines. The flow of the discussion covers salient points of the algorithms without necessitating a technical deep dive. This makes the book more accessible to people from disciplines other than just Computer Science.

The chapter titles are imaginative and serve to hook the interest of the reader. In addition, the chapter titles segue nicely into the discussions per chapter.

For example, the first chapter is titled "Stock Spans." The chapter starts with a discussion of how stock spans are solvable in several ways, depending on the constraints identified. This is a great jumping off point to discussions of how we can determine which algorithms would serve us better. Also the problem is basic enough that a discussion of basic structures fits well.

2 Chapter 1. Stock Spans

While working on the problem identified, the basic data structures (i.e. arrays, and stacks) are introduced. The discussion goes into complexity theory and orients the reader with the concepts related to it.

3 Chapter 2. Exploring the Labyrinth

The introduction to graph theory is started within the context of trying to solve a traversal of a labyrinth. The progression from identifying the basic elements of graphs to the different kinds of graphs and their representations is a logical and smooth transition. The section ends with discussions on depth-first and breadth-first traversals.

4 Chapter 3. Compressing

The chapter focuses on Huffman Coding using priority queues with a hint on using an array implementation. Then the chapter ends with an exposition of the Lempel–Ziv–Welch Compression.

5 Chapter 4. Secrets

To start the chapter off, a decryption challenge is given to the user. There is the introduction of the use of letter frequency tables to decrypt the message. From there, the one-time pads are discussed before going into the AES Cipher. The chapter ends with a discussion of the Diffie–Hellman Key Exchange.

Unfortunately, in the latter part of the chapter, it is not my forte so I can't hazard a guess on the veracity of the presentation. But from my meager background on the matter, I thought the presentation of the concept was adequate for the uninitiated to get some understanding of the concepts involved.

6 Chapter 5. Split Secrets

Public key cryptography is the focus of this chapter. The chapter starts with a good presentation of the idea behind the cryptographic system and then goes into a discussion of RSA. The latter part of the chapter touches on the application of cryptographic systems to the support of internet traffic anonymization in the view from Tor.

7 Chapter 6. Tasks In Order

The chapter goes into graph theory emphasizing directed acyclic graphs, the application/use of topological sorts, weighted directed graph representations and critical paths. The graphical representations chosen were very helpful in the discussion.

8 Chapter 7. Lines, Paragraphs, Paths

On this one, it is all about the shortest path problem. It starts off with how to go about solving word wrapping in paragraphs - and how it can be looked at as a shortest path problem. Djikstra's algorithm is discussed along with the algorithm's characteristics.

9 Chapter 8. Routing, Arbitrage

The topics in the previous chapter are moved further along by discussing the Bellman–Ford–Moore Algorithm. Internet routing (and a bit of a segue on the protocols used in the Internet) is covered in the initial section.

10 Chapter 9. What's Most Important

Web search for relevant pages in the Internet is the problem that is raised – how to effectively rank web pages in order to infer their significance to a query. The chapter delves into PageRank, along with the Power Method and the Google Matrix.

11 Chapter 10. Voting Strengths

Different voting methods are covered, emphasizing how they change the interpretation of the results as to voter preferences. It is presented that this is also a graph issue that involves the strongest path. And, of course, algorithms are discussed regarding calculating the strongest paths.

12 Chapter 11. Brute Forces, Secretaries, and Dichotomies

In this chapter, discussions are included on searching algorithms and the mathematical concepts that relate to their characteristics or behaviors. Sequential search is covered, as well as binary search logic and the strength of the divide and conquer approach.

13 Chapter 12. A Menagerie of Sorts

The fundamental sorting routines are presented: selection, insertion, heap, merge, and quicksort. The thing that I liked about how these algorithms are presented is that there is an emphasis on when you should use particular algorithms, aside from just talking about time complexity. The intention, as indicated from the start by the author, is for a more general audience, and I felt that this is actually a good point to make. For would-be implementers, the discussion should help with making a pragmatic choice on a sorting algorithm to use.

14 Chapter 13. The Cloakroom, the Pigeon, and the Bucket

After the discussion of sorting algorithms, the next logical concept to cover would be hashing, hash tables, buckets and hashing functions. I liked the discussion regarding what makes for good hashing functions – and why some schemes are better than others. Collision and resolutions/behaviors related to it are delved into – with explicit algorithms presented on fundamental operations on the hash table with chained lists.

The concept of using hash tables to digitally fingerprint data is an interesting example.

Bloom filters, how they were useful, and how they are connected to hash algorithms, are discussed.

15 Chapter 14. Bits and Trees

The next topics are classification and decision trees. Divination and the use of the I Ching hexagrams at the start of the chapter is an interesting choice. Further topics include outcomes and probabilities, entropy, classifications, computation of information gain, and Occam's Razor! This particular chapter was explained well, but might be a little on the heavy side due to the necessity to discuss it in some depth in order to get a good grounding on the concepts.

16 Chapter 15. Stringing Along

After presenting a brute force text searching algorithm, the use of the Knuth–Morris–Pratt algorithm for string searching/matching is explained. There is a considerable amount of good visualization done to help understand the concepts. The chapter ends with a presentation of the Boyer–Moore–Horspool algorithm.

17 Chapter 16. Leave To Chance

The book ends with a discussion of the concepts of randomness, random number generation, random sampling/subset generation, probabilities, and working with prime numbers (searching for primes and the Sieve of Eratosthenes).

18 Opinion

All of the chapter discussions are done in a very effective manner. Interesting and relevant examples and case studies are presented to start off each chapter. The chapters provide good coverage of the discussion points raised. But as the author indicated, the plan was not a deep discussion but an attempt to provide solid grounding. And I think for the most part the text has done what was intended.

The use of pseudocode to present algorithms in the discussions made sense, as it removes any reliance on language-specific constructs in the presentation. It made the focus on ideas more direct.

At times though, it would have been nice if there were more subsection headers to delineate the content more – in case one needed to reference back to particular sections or ideas.

The "Notes" section at the ends of chapters provided points for further study in a very accessible manner.

Joint Review of[4]
Quadratic Residues and Non-Residues
by Steve Wright
Springer, 2016
292 pages, Softcover, $59.90

and

The Quadratic Reciprocity Law
by Oswald Baumgart
Edited and translated by Franz Lemmermeyer
Springer, 2015
172 pages, Hardcover, $89.99

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

> *"Theorema fundamentale, quod sane inter elegantissima in hoc genere est referendum, in eadem forma simplici, in qua supra propositum est, a nemine hucusque fuit prolatum." – C. F. Gauss*

Let p be a prime. An element $a \in \mathbb{Z}_p$ is said to be a quadratic residue if it is a square, i.e., iff for some $b \in \mathbb{Z}_p$, we have $a \equiv b^2 \pmod{p}$. Now let p, q be distinct odd primes. The Law of Quadratic Reciprocity (LQR) says:

> Let p be an odd prime, and a a natural number not divisible by p. If q is prime such that $p = \pm q \pmod{4a}$, then a is a quadratic residue mod p iff it is a quadratic residue mod q.

The "reciprocality" of this law is already evident in this form, which is more or less as set down by Euler, expressed here in modern notation. But it is more plainly and beautifully obvious thanks to Legendre (who was responsible for the word "reciprocity" in this context), via the symbol that bears his name:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p|a \\ 1 & \text{if } a \text{ is a quadratic residue mod } p \\ -1 & \text{if } a \text{ is a quadratic nonresidue mod } p. \end{cases}$$

In these terms, LQR becomes simply,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

In his *Disquisitiones Arithmeticæ,* quoted above, Gauss called it the "fundamental theorem" that "must certainly be regarded as one of the most elegant of its type."[5] In private, he dubbed it the "*Theorema Aureum*," the "Golden Theorem." The law itself, its many proofs, its implications and generalizations, its influence on the advancement of number theory, and the underlying history, are deep and fascinating.

[4]

[5] And goes on to say, "[and] no one has thus far presented it in as simple a form as we have done above."

But why is LQR so important? Gauss came up with no fewer than 8 distinct proofs, and mathematicians after him quickly followed with dozens more. The theorem itself has many motivations, but a central goal driving Gauss's and subsequent work was the search for higher reciprocity laws. Thus as Wright says in his book, LQR "has inspired, by far, more proofs than any other theorem of number theory." While the upwards of 300 proofs on record (through 2014, and probably still counting; see the discussion of Baumgart/Lemmermeyer below) are not all completely distinct, there is a striking diversity of techniques leading to very different generalizations, which led to important developments in algebraic number theory, a crowning achievement of 19th-century mathematics and a vital ongoing area of research. Furthermore, LQR in particular and quadratic residues in general have numerous applications, including many computational ones, notably in cryptography. In even greater generality, algebraic number theory has numerous applications in theoretical computer science (see, e.g., [Sh] or [TW]).

The two books under review are based on the same topic, but while they overlap considerably, there is a substantial symmetric difference. For one, Baumgart's "The Quadratic Reciprocity Law" was written (in German) in 1885, and the present volume is a recent English translation by Lemmermeyer. It includes proofs that are not in Wright's book. By contrast, Wright's book "Quadratic Residues and Non-Residues" was written within the past couple of years, and while it doesn't give as many different proofs of LQR, it is much broader in scope, and deals with very recent and even ongoing research. I do not mean to imply any qualitative or quantitative comparisons here whatsoever; both books possess their own unique, independent facets and qualities. Rather, it seemed fitting to consider the two under the same review, in view of the common theme, as well as the depth and enduring interest that the subject offers.

To cut to the chase, these two books are welcome and valuable contributions, providing different perspectives, to the extensive literature on this important subject. One can learn a great deal from either one, and even more from both. For the remainder of this review I consider each book in turn.

1 Wright

1.1 Overview and Summary of Contents

To borrow (and slightly re-arrange) some of the author's own words, this book uses the study of quadratic residues and non-residues as a "window through which to view the development... of many of the key ideas and techniques that are used everywhere in number theory today." Quadratic reciprocity together with its numerous proofs and generalizations has employed and/or led to diverse concepts in algebraic and analytic number theory. Indeed, the text introduces and expounds on many central topics in these areas. The following detailed summary of concepts should convey how this is done.

1. Chapter 1, Introduction: Solving the General Quadratic Congruence Modulo a Prime. A brief chapter stating the ideas of quadratic congruence and setting notation.
2. Chapter 2, Basic Facts: Introduces essential facts about residues and non-residues, the Legendre symbol (written as a character $\chi_p(x) = \left(\frac{x}{p}\right)$) and its multiplicative properties, and important results such as Gauss's Lemma (see discussion of Baumgart/Lemmermeyer for a statement) and Euler's Criterion. Two problems are then posed. The "Basic Problem" is, given an integer $d \in \mathbb{Z}$, to determine for which primes p is d a quadratic residue mod p. The author explains, via examples and drawing on multiplicative properties of the Legendre symbol, how the Basic Problem reduces to the "Fundamental Problem." The latter is, given a *prime* q, to determine the set of primes p for which q is a residue, as well as the set of primes for which q is a non-residue. In this chapter, the quadratic character $\chi_p(2)$

is computed, and hence these problems are solved for $q = 2$. Both problems are solved in Chapter 4 for odd primes.

3. Chapter 3, Gauss' Theorema Aureum: The Law of Quadratic Reciprocity. The chapter begins with a discussion of reciprocity laws in general, at first motivated by the question of which integers can be written as a sum of two squares (a question answered by a well-known theorem of Fermat). Next the theorem is posed, and then, in the context of a historical discussion, an equivalent formulation is given (the one due to Euler that was stated at the beginning of this review). Next, we proceed with five distinct proofs of LQR (two more are given in Chapters 7 and 8, respectively). The first, a variant, due to Eisenstein, of Gauss' third proof, uses Gauss' Lemma in conjunction with an appealing geometrical argument. The second also relies on Gauss' Lemma, but instead proves the equivalent formulation of LQR due to Euler. We move on to a proof using Gauss sums (my personal favorite), which in turn requires a quick (compressed but cogent) introduction to algebraic numbers and algebraic number fields. The next proof, via the theory of ideals in the ring of algebraic integers in a quadratic number field, is quite a bit more involved and requires considerable mathematical machinery that cannot be realistically included in the text. This covers a lot of ground, one crucial ingredient being Dedekind's theorem of unique factorization into prime ideals, which is proved later, in Chapter 5. Necessary facts about the ideal class group and its structure, and the norm and trace functions, are primarily stated without proof, referring the reader to Hecke's classic lecture notes [He] on algebraic number theory. The non-self-containment of the exposition is used to some advantage, since (assuming one is willing to accept this much on faith), by presenting the "big picture," it saves one the trouble of working through the bulk of Hecke's work (which, emphatically, is not to say it isn't worthwhile reading!). The presentation appears at this point in the text, as it represents (in a more modern formulation) Gauss' second proof of LQR based on his theory of genera of quadratic forms. The connection between that formulation and the modern one (a theme taken up again in Chapter 8) is summarized at the end of this part. Finally, the chapter ends with a proof of LQR via Galois theory, following ideas originally due to Kronecker. As with the material on ideal theory, a prior acquaintance with Galois Theory would be advantageous, but there is much less to take on faith for this proof.
4. Chapter 4, Four Interesting Applications of Quadratic Reciprocity: As promised in Chapter 2, the first application is the complete solution to the Basic Problem (via the Fundamental Problem, supplemented by the Method of Successive Substitution as a key ingredient), also illustrated by example. At this point the author points out the connection between the Fundamental Problem and Dirichlet's Theorem on Primes in Arithmetic Progressions, which is discussed later in the chapter. Indeed, the second (somewhat surprising) application, that any finite set of integers is a set of quadratic residues for infinitely many primes, follows in a relatively straightforward way from Dirichlet's theorem. The proof of that theorem is not included but is very clearly discussed, including a treatment of Dirichlet characters and the Dirichlet L-functions (taking the opportunity to mention the Riemann zeta function and the Riemann hypothesis). A refinement follows, in which the *density* of prime residues of a finite set is computed from scratch, except for reliance on the Prime Number Theorem for primes in arithmetic progressions. The chapter concludes with a complete account of the Feige-Fiat-Shamir zero-knowledge identification scheme. This provides a good opportunity for introducing several important concepts. These include the Jacobi symbols and their reciprocity law, whose proof is included. These in turn are required for the efficient computation of the Legendre symbols without the need to factor, a key element of the protocol; this is also explained and illustrated with examples.
5. Chapter 5: The Zeta Function of an Algebraic Number Field and Some Applications. The nominal agenda of this chapter is to prove a result stated in the previous one (I say "nominal" because proving

that result takes us, again, into deep territory). That goal is to determine when a finite set S is a set of *non*-residues of infinitely many primes. In fact, this holds if and only if any product of an odd number of elements of S is not a square; the hard part being to establish the "if" direction of this equivalence. For the sake of later discussion, it's convenient to state the theorem here more precisely:

Theorem (4.12): A finite set $S \in \mathbb{N}$ is a set of non-residues of infinitely many primes iff for any $T \subseteq S$ of odd cardinality, $\prod_{i \in T} i$ is not a square.

The first result stated (without proof) is Dedekind's Ideal Distribution Theorem, which quantifies the cardinality $Z(n)$ of the set of ideals in a ring (of the algebraic integers of a number field) whose norm is bounded above by n. Drawing again on the ideal class group and some references to Hecke [He], it is proved that $Z(n)$ is finite. Dedekind's theorem gives an asymptotic expression for $Z(n)/n$ in terms of a number of important parameters of the number field, e.g., the discriminant and the regulator, which are explained but not explored in detail. The theorem is specialized to the case of quadratic number fields (a result first due to Dirichlet), which suffices for the main results of the chapter. The Dedekind-Dirichlet zeta function is then introduced, its convergence proved, the Euler-Dedekind product formula given, and its factorization over rational primes (analogous to the Euler product expansion for the Riemann zeta function). After specializing these to the case of quadratic number fields, especially to obtain a convenient product expansion in that setting, the groundwork is then laid for the main result of the chapter, namely Theorem 4.12 as stated above. In addition, the density of those primes is determined, and some related results are presented. Prominent among these is a strengthening of Theorem 4.12, which characterizes which patterns of residues/non-residues in a finite set are "supported" by an infinite number of primes:

Theorem (5.13): Given a finite set $S \in \mathbb{N}$, for any given function $\varepsilon : S \to \{-1, 1\}$, the set $\{p | p$ is prime and $\chi_p \equiv \varepsilon\}$ is infinite if and only if for any $T \subseteq S$, $\prod_{i \in T} i$ is not a square.

The chapter concludes with a proof of the Fundamental Theorem of Ideal Theory, which was needed in the proof of the Euler-Dedekind product formula, as well as in the earlier ideal-theoretic proof of LQR in Chapter 3, albeit in that case in a weaker form.

6. Chapter 6: Elementary Proofs. In this relatively brief chapter, proofs of Theorems 5.13 and 4.12 are presented using "elementary" techniques of combinatorics and linear algebra, rather than analytic techniques based on zeta functions.

7. Chapter 7: Dirichlet L-Functions and the Distribution of Quadratic Residues. This chapter addresses the problem of comparing the number of residues and non-residues contained in an interval. A critical fact about the Dirichlet function $L(s, \chi)$ in the proof of his Theorem on Primes in Arithmetic Progressions was the simple inequality $L(1, \chi) \neq 0$, for any non-principal Dirichlet character χ (i.e., any non-trivial character that does not send all elements to 1). A key result proved in this chapter is that if χ is *real* and non-principal, then we actually have that $L(1, \chi)$ is real and *positive*. This, in turn, implies that sums of Legendre symbols contained in certain intervals are positive. Indeed, it turns out that the values of these sums are positive multiples of $L(1, \chi)$ for real non-principal χ. (I, for one, find it amazing how much you can get out of $L(1, \chi) > 0$!) Proving these facts occupies most of the chapter. Along the way we encounter some results and ideas that are interesting in their own right. One is determining the sign (not just the magnitude) of the quadratic Gauss sum, a problem which Gauss himself famously took four years to solve. Another is a quick summary of the basics of complex analysis (not assumed to be in the reader's background), including the idea of analytic

functions over $\mathbb{C}$, contour integration, Cauchy's Integral Theorem, and the Residue Theorem. There is a section on the convergence of Fourier series to periodic, piecewise differentiable functions. All these techniques are used in the lengthy and carefully presented proof of the main theorem of the chapter, following a method due to Berndt. There follows an elegant proof of $L(1,\chi) \neq 0$ (which is used to derive $L(1,\chi) > 0$), due to de la Vallée Poussin, using little more than analytic properties of the Riemann ζ-function and the Euler product expansion. The chapter concludes with yet another proof of LQR, based on finite Fourier series and Gauss sums.

8. Chapter 8: Dirchlet's Class-Number Formula. This chapter presents another proof of $L(1,\chi) \neq 0$, which provides deeper insight into why it is true. The treatment returns to the theory of quadratic forms, as discussed late in Chapter 3. The idea is to classify irreducible, primitive quadratic forms according to their discriminants. These forms are partitioned into equivalence classes, where the equivalence is defined via modular substitutions. Roughly speaking, the number of classes as a function of discriminant is referred to as the class number. Dirichlet's Class Number Formula ("DCNF") expresses $L(1,\chi)$ in terms of the class number. Thus the fact that $L(1,\chi) \neq 0$ is a consequence of the nonzero number of objects (classes) it is effectively counting, an insight lacking in the analytic proof of de la Vallée Poussin. A key result in the proof of DCNF is another formula, expressed as certain sums of Dirichlet characters, this time for the number of ways $R(n)$ of representing a given integer by quadratic forms. That proof is not given, but the elegant proof of the DCNF is presented at length, which is based on two ways of estimating $R(n)$, one algebraic and other geometric. Of course the class number for quadratic forms is closely related to the class number of ideal classes in quadratic number fields, and thus the DCNF also allows us to count those ideal classes, as explained in this chapter. The chapter concludes with one last proof of LQR, this one based on Gauss sums with Dirichlet characters and the structure theory for such characters.
9. Chapter 9: Quadratic Residues and Non-residues in Arithmetic Progressions. This chapter concentrates on previously published original research of the author. A result of Davenport says that arbitrary length sequences of *consecutive* quadratic residues (and non-residues) mod a given prime p occur in the interval $[1 \ldots p-1]$. Even the number of such sequences of residues/non-residues approaches infinity as $p \to \infty$. Wright generalizes these results to show similar results for arbitrary length *arithmetic progressions* of residues/non-residues, and in a further generalization, to unions of distinct such arithmetic progressions. The techniques are quite interesting, and build on estimates of both complete and incomplete Weil sums. These are sums of additive characters (Legendre symbols) evaluated at values of certain polynomials, and their evaluation also entails estimates of hybrid sums that combine additive and multiplicative characters. Reducing the stated problems to these estimates requires rather elaborate arguments in combinatorial number theory, which are amply explained. Some concrete examples are provided to illustrate the results as well as the techniques.
10. Chapter 10: Are Quadratic Residues Randomly Distributed? In this final relatively brief chapter evidence is presented that the answer is "yes." First some of the numerical evidence is presented. More convincingly, based on a result of Davenport and Erdős, it is proved (using the Weil sum estimates of chapter 9) that the relevant character sums ("quadratic excesses," introduced in Chapter 7) satisfy an appropriate central limit theorem.

1.2 Opinion

There are many textbooks that cover most of the material treated in this book. Although I can't profess to have an extensive knowledge of those sources, I believe that the treatment here is unusual. In particular,

it begins with the very basic elementary number theoretic ideas of quadratic residues and non-residues, and proves LQR via elementary means. Motivated by this, it then ascends to ever-increasing levels of sophistication, which brings the reader to an understanding of many important concepts in analytic and algebraic number theory. While it provides copious detail on all the proofs, at the same time it serves very well to provide a panoramic view of the subject, which enables one to understand both the reason certain concepts were introduced as well as how they evolved historically. There are other books that do something like this. Two that easily come to mind are Ireland and Rosen [IR] and Goldman [Go]. The latter especially takes a deliberately historical approach. However, both of those volumes treat number theory broadly conceived (albeit with certain sets of emphases), and do not use any one single idea (as in this case, quadratic residues) around which to build a narrative. As I have intimated previously on this column, I believe there is great pedagogical value in drawing on a small number of examples for motivation. Given a theorem with such broad impact as quadratic reciprocity, a single example suffices very well!

The book does have shortcomings, but given its goals, they are minor. It may not serve well as a formal textbook, since it has no exercises *per se*. On the other hand, as usual, almost every page is rich with implicit exercises to fill in the steps that are inevitably left out, and there are numerous points in the text where the author explicitly suggests the reader provide proofs that have been omitted. I think its most optimal role would be as the author originally intended it, as the basis of a seminar or readings course. It can certainly be used effectively at the advanced undergraduate or beginning graduate level, for students who have had a solid background in algebra, and a certain amount of elementary number theory would help. The book is also, as mentioned above, not entirely self-contained. This is both an advantage (accept the claims that are made, and you can attain insightful overviews of the proofs of some very significant theorems) and a disadvantage (not everything can be proved without a significant amount of outside reading). As for the latter, I found that keeping Ireland and Rosen [IR] and Hecke [He] at hand provided more than adequate support.

In short, I found reading this book to be a very rewarding experience, and I think any determined reader can reap similar benefits.

2 Baumgart/Lemmermeyer

2.1 Overview and Summary of Contents

Oswald Baumgart wrote his thesis *Über das quadraticshe Reciprocitätsgesetz. Eine vergleichende Darstellung der Beweise*[6] in Göttingen in 1885. One can hardly improve on quoting him in full (in Lemmermeyer's translation) on his intended goal:

> In the following we will present all known proofs of the quadratic reciprocity law and carefully compare the principles on which they are based. The author believes that such a first comparison is not completely useless, because this law is the fundamental result in the theory of quadratic residues and nonresidues, moveover because the principles on which they are built allow us to find new and very general methods, and finally because the proofs of this law have induced a very welcome interaction between some, until then almost or completely isolated, areas of mathematics. In addition, the history of this theorem is a faithful reflection of the simultaneous history of mathematics in the small.

[6] "On the Quadratic Reciprocity Law. A Comparative Presentation of its Proofs"

Baumgart's thesis is divided into two parts. The first and longer part (Chapters 1 through 8) is a presentation of the various proofs. The second part (Chapters 9 through 14) is a comparative presentation of the principles on which the proofs are based, often amplifying or clarifying aspects of the preceding proofs. In Chapter 15, Lemmermeyer provides a meticulously referenced list of proofs through 2014, at that time 314 in number. Here is a summary of the contents of Baumgart's chapters. Rather than provide detailed summaries of the Part II chapters, I find it more natural to refer ahead to them (as appropriate) in discussing the Part I chapters. Of course, unless otherwise stated, all results are those treated by Baumgart, and hence are no later than 1885.

Part I:

1. Chapter 1: From Fermat to Legendre. A quick setup of notation, and a brief historical survey.

2. Chapter 2: Gauss' Proof by Mathematical Induction. This is Gauss's first proof, an inductive proof by cases, which seems quite ungainly[7] in comparison with subsequent proofs (including those by Gauss). There are 8 cases, but they can be quickly reduced to only 2 essentially different ones. As Baumgart points out in Chapter 9, the proliferation of cases was in part an artifact of Gauss's notation. The induction is on q, with the assumption (wlog) that $q > p$.

3. Chapter 3: Proof by Reduction. As explained in Chapter 10, the proofs presented in this chapter are all based on Gauss's Lemma (which is what Baumgart means by "reduction"). Gauss's Lemma[8] states that $\left(\frac{p}{q}\right) = (-1)^{\mu}$, where μ is the number of "least residues," i.e., integers between $-p/2$ and $p/2$ which are congruent mod q to one of the elements in the sequence $p, 2p, 3p, \ldots, \frac{q-1}{2}p$. The proofs given include Gauss' third and fifth proof, and Eisenstein's geometric proof (based in part on Gauss' third; cf. my discussion of Wright, Chapter 3). There are a number of others, including one by Stern which Lemmermeyer points out is not correct, but still contains valuable ideas. Again as Baumgart explains in Chapter 10, these proofs are distinguished in a number of ways, e.g., some of them use different "half systems" (i.e., sequences $a_1, \ldots, a_{(q-1)/2}$ mod q). It's worth noting that Baumgart's categorization in these chapters cannot be exact. For example, Gauss's Lemma is used in proofs in other chapters, e.g., in Liouville's proof in Chapter 5 based on cyclotomy.

4. Chapter 4: Eisenstein's Proof Using Complex Analysis. This presents one proof, the ingenious and compact argument due to Eisenstein based on the sine function. Further detail is given in Chapter 11. (This is a standard treatment of the proof, although it is not obvious, at least to this reader, what is "complex" in the proof as presented. It is made very explicit in a version given in Ireland and Rosen [IR], which utilizes properties of roots of unity.)

5. Chapter 5: Proofs Using Results from Cyclotomy. Here the role of complex numbers is critical, the unifying theme being Gauss sums and related quantities. The chapter includes Gauss's seventh proof (also Lebesgue's second) based on quadratic periods of the cyclotomic equation; Gauss's fourth and sixth proofs, and proofs by Cauchy, Jacobi, and Eisenstein, all based on Gauss sums, including the determination of the sign; another proof by Eisenstein based on what came to be known as (multiple) Jacobi sums; and others. Among the most interesting techniques in this regard are analytical, due to Dirichlet and Cauchy, discussed in Chapter 12: Cauchy discovered that the sign of the Gauss sum

[7] Despite many years of not attracting much interest, in modern times some of its ideas were used by Tate for calculations in K-theory, cf. [Go], pg. 153.

[8] That is to say "What is Known as Gauss's Lemma in This Context"; for there are at least two others!

emerges in transformations of theta functions, and Baumgart describes the close connection between this and Dirichlet's technique.

6. Chapter 6: Proofs Based on the Theory of Quadratic Forms. These are the proofs based on equivalence classes of quadratic forms with a given discriminant. As in Wright's book, due to its complexity Baumgart omits that part of the theory that would be required to prove all the necessary lemmata. The lemma on the number of genera is stated without proof, and Gauss's second proof of LQR takes off from there. Given that, the proof is remarkably elegant. Kummer's first proof is based a Pell equation. His second proof is based on properties of primes represented by quadratic forms. As Lemmermeyer points out in his notes to Chapter 13, these proofs have been translated into the modern language of ideals in algebraic number fields (cf. the discussion of the later sections of Chapter 3 in Wright).

7. Chapter 7: The Supplementary Laws of the Quadratic Reciprocity Law and the Generalized Reciprocity Law. The expert or extremely alert reader knows by now that I lied (in the interest of succinctness, of course) at the outset of this review. There are two "supplements" to LQR, which determine the quadratic characters of -1 and 2, namely $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ and $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. This chapter proves these laws via various techniques as in preceding chapters, e.g., reduction, cyclotomy and quadratic forms. The LQR is then generalized to negative primes and further, with the help of the Jacobi symbol, to composites.

8. Chapter 8: Algorithms for Determining the Quadratic Character. LQR can be used in a straightforward manner to compute efficiently the value of the Legendre symbol. Another method for this is via continued fractions, and most of the algorithms given here fall under that second heading.

Part II:

9. Chapter 9: Gauss's Proof by Induction. (See comments on Chapter 2.)

10. Chapter 10: Proofs by Reduction. (See comments on Chapter 3.)

11. Chapter 11: Eisenstein's Proofs Using Complex Analysis. (See comments on Chapter 4.)

12. Chapter 12: Proofs Using Results from Cyclotomy. (See comments on Chapter 5.)

13. Chapter 13: Proofs Based on the Theory of Quadratic Forms. (See comments on Chapter 6.)

14. Chapter 14: Final Comments. This is mainly historical in nature, with an emphasis on chronology and priority, and includes a list of proofs known in Baumgart's time.

Throughout the book, in footnotes, Lemmermeyer is careful to resolve ambiguities, translate into modern mathematical language when that is helpful, or point out errors in the original. In addition, he includes notes at the ends of some of the chapters, primarily in Part II, with citations to the appropriate literature.

2.2 Opinion

One clear virtue of this book is as a historical record of progress on quadratic reciprocity, at least through the course of most of the 19th century. The mathematician L. E. Dickson intended the entire 4th volume of his already monumental 3-volume history of number theory [Di] to cover reciprocity laws. His student was to have written it, and may very well have produced a manuscript, but due to a combination of unfortunate circumstances, that volume never came to fruition (the interesting story is recounted at length in [Fe], one

of the many tidbits I learned from the Baumgart/Lemmermeyer book). Part of Lemmermeyer's motivation in producing this translation is as a first step towards filling this gap in the record.

However, it is far more than a document of purely historical interest. It contains the details of many important proofs, and it is fascinating to see how relevant many of them remain to the present day. A number of the proofs are not the among the canonical ones you will find in textbooks, and it's always interesting to see the alternatives, which (one never knows) may prove useful to modern researchers in unpredictable ways.

References

[Di] L. E. DICKSON, *History of the Theory of Numbers,* AMS Chelsea Publishing, Volumes I-III, AMS Chelsea Publishing, New York, reprinted 1992.

[Fe] D. FENSTER, "Why Dickson Left Quadratic Reciprocity out of his History of the Theory of Numbers," *Amer. Math. Monthly* **106** (1999), pp. 618-627.

[Go] J. R. GOLDMAN, *The Queen of Mathematics,* A K Peters, Wellesley, 1998.

[He] E. HECKE, *Lectures on the Theory of Algebraic Numbers,* (translated from the German original of 1923 by G. U. Brauer and J. R. Goldman), Vol. 77 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2010.

[IR] K. IRELAND AND M. ROSEN, *A Classical Introduction to Modern Number Theory*, Vol. 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[Sh] V. SHOUP, *A Computational Introduction to Number Theory and Algebra*. Cambridge University Press, Cambridge, 2005.

[TW] W. TRAPPE AND L. C. WASHINGTON, *Introduction to Cryptography with Coding Theory*. Pearson/Prentice-Hall, Upper Saddle River, 2006.