Review of the book

Fundamental Number Theory with Applications

(Second Edition)

by Richard A. Mollin

CRC Press, Taylor & Francis Group, 2008

ISBN: 978-1-4200-6659-3

Francesco Sica
University of Calgary

15 March 2010

1 Overview of Book

This is an introductory text in number theory from a well-known name among Canadian number theorists, at the level of an undergraduate course in a mathematically oriented curriculum in a North American university and indeed it covers most of the material traditionally expected in such a course. Although the reviewer is not acquainted with the first edition of the book, the author summarizes in the preface the changes that occurred in the second edition. These consist for the most part in the addition of topics which, although quite classical, do not get so widespread a coverage at the undergraduate level. For instance, let us mention the theory of partitions, the use of generating functions, primality testing and factoring and special diophantine equations like Bachet's. There are a few deletions or relegations to the appendix, for instance with Appendix A, which deals with prerequisites (discrete mathematics and calculus, as well as some linear algebra).

2 Book Summary

The table of contents runs as follows (I have written the titles of sections on the same line as the chapters headings):

① Arithmetic of the Integers: induction, division, primes, the Chinese remainder theorem, Thue's theorem, combinatorial number theory, partition and generating functions, true primality tests, distribution of primes

② Modular Arithmetic: basic properties, modular perspective, arithmetic functions (Euler, Carmichael, Möbius), number and sum of divisors, the floor and the ceiling, polynomial congruences, primality testing, cryptology

③ Primitive Roots: order, existence, indices, random number generation, public-key cryptography

④ Quadratic Residues: the Legendre symbol, the quadratic reciprocity law, factoring

⑤ Simple Continued Fractions and Diophantine Approximation: infinite simple continued fractions, periodic simple continued fractions, Pell's equation and surds, continued fractions and factoring

⑥ Additivity — Sums of Powers: sums of two squares, sums of three squares, sums of four squares, sums of cubes

⑦ Diophantine Equations: norm-form equations, the equation $ax^2 + by^2 + cz^2 = 0$, Bachet's equation, Fermat's last theorem

Appendix A Fundamental Facts

Appendix B Complexity

Appendix C Primes ≤ 9547 and Least Primitive Roots

Appendix D Indices

Appendix E The ABC Conjecture

Appendix F Primes is in P

There are still the few usual last entries (bibliography, index, list of symbols and about the author). Note the pedagogical and customary (in North America) section of solution to odd-numbered exercises.

3 Reviewer's Comments

3.1 Critical Description of Chapters

① In this first chapter we take off rather smoothly and in a conventional way, until we hit Thue's theorem (an application of Dirichlet's box principle or pigeonhole principle), which is mainly used as a lemma in the representation of primes as linear combination of squares (for instance in the famous Fermat theorem that an odd prime p is expressible as a sum of two integral squares if and only if it has remainder 1 when divided by four). I find this choice a bit artificial, a more natural one (without the use of new techniques) would have been to use something like Cornacchia's algorithm, which is also constructive (i.e. gives a polynomial-time algorithm to find the two squares in Fermat's theorem for instance). The choice of the Thue theorem is unique, from what I am aware of.

Note the elegant use of examples taken from historical textbooks (the coconut problem, the egg-basket problem). Indeed the breadth and depth of the author's knowledge are pervasive and is one of the features of this monograph that will beckon the curious reader.

The section on combinatorial methods could have been done without. The author is striving to handle a few results (for instance Wilson's and Fermat's little theorems) without introducing modular arithmetic yet (it will be done in Chapter 2) and therefore encumbering himself with heavy notations.

I have also noticed that, in light of the audience but with a view towards educating to the modern practice, the author has come midway in some notation, for instance, with $\log_e$ to denote the natural logarithm (that students will have encountered as ln in first-year calculus whereas number theorists universally use log).

② The first two sections are devoted to the introduction of modular arithmetic and restatements of some proved results in this new language. It would have saved space if these had been introduced before, although I recognize that modular arithmetic does sweep some important information under the carpet.

In the primality testing section, the Miller-Rabin (more correctly, as the author points out, the Miller-Selfridge-Rabin) probabilistic test is introduced (although its success rate is not analyzed).

The cryptology section deals with historical cryptography (polyalphabetic block ciphers and stream ciphers)

③ Most of the material here is standard. The section on public-key cryptography deals with Pohlig-Hellman (based on the discrete log problem) and RSA (based on the difficulty of factoring) encryption. Three "random" number generating algorithms are presented, without of course proving anything about their randomness.

④ In this chapter, the proof of the quadratic reciprocity law is the "geometric" proof obtained by counting the number of some lattice points inside a rectangle. Factoring methods like Fermat's or Pollard's $p-1$ and Rho are introduced.

⑤ I will only mention here the last section, which is the culmination of the efforts of the whole chapter. Fermat's method is developed into the continued fraction method for factoring. Unfortunately, the author does not mention anything about more sophisticated methods, except that they are "beyond the scope of this book", together with a reference for the interested reader.

⑥ All the sections except the last one are classical (the sum of 3 squares is usually skimmed, since it is in a much more difficult class to attack, and no exception is made here). The sum of cubes section is more interesting and contains a result about the existence of a representation of rational numbers as sums of three rational cubes. In this section as well as the next chapter, the author shows great skills at algebraic manipulations to solve equations of special types, much akin to problem solving in mathematical competitions (indeed, the reviewer has seen similar examples as challenges in the specialized press). A nice complement to this chapter would have been to point out recent developments (1998 and 2001 respectively) in the representation of primes as a square plus a fourth power by Friedlander and Iwaniec and as a cube plus twice another cube by Heath-Brown.

3.2 The Use of Biographical Sketches

One of the most interesting features of this book is the extensive (and crunchy) biographical sketches of relevant mathematicians (both living and dead). There is one notable omission, though. Wiles only has a couple of lines in the cartouche on Fermat's last theorem. I believe he deserves a full biography in this book, since it is also his achievement which is likely to draw many young recruits to this venerable branch of mathematics.
There are also some typos in the names of mathematicians (like an English spelling of Nicholas instead of Nicolas for De La Vallée Poussin, or more unfortunately, Sophie Germane instead of Germain).

3.3 The Selection of Exercises

The exercises are varied and for the most part, classical. However, I shall deplore the difficulty rating system. In my view, there are many more exercises to be starred, especially among those in the final chapters. Even bright undergraduates would be at a loss in attempting to solve them.

4 Reviewer's Recommendation

I heartily recommend this book to undergraduates and the passing layman, as it is the work of a master and is lucidly explained. Most of the treatment can be also found elsewhere, but the biographical notes are definitely enticing. This book has a sequel devoted to more advanced aspects of the theory, which are only briefly mentioned in the preface.
The reviewer is a visiting professor of Mathematics at the University of Calgary.