Review of the book

Advanced Number Theory with Applications

by Richard A. Mollin

CRC Press, Taylor & Francis Groups 2010

ISBN: 978-1-4200-8328-6

Fan Junjie Bertrand
Centre for Strategic Infocomm Technologies

30 May 2011

1 Overview of Book

This is the sequel to the introductory text 'Fundamental Number Theory with Applications' written by a well-known leader in algebra and number theory. Suitable for advanced undergraduates and beginning graduates in mathematics, this text offers a sweeping introduction across a wide range of algebraic, analytic, combinatorial, cryptographic, and geometric aspects of number theory and some of their applications. Indeed, this text starts off with algebraic number theory, binary quadratic forms, and Diophantine approximation, and ends with an overview of Fermat's Last Theorem, and numerous consequences of the ABC conjecture, including the Thue-Siegel-Roth Theorem, the Erdos-Mollin-Walsh conjecture and the Granville-Langevin Conjecture. Numerous extensive biographical sketches of relevant mathematicians are also scattered throughout the book.

2 Book Summary

The first chapter contains a standard introduction to the necessary basic on algebraic number fields. But it has a special view towards quadratic fields and the applications to solutions of the Ramanujan-Nagell Diophantine equations, factorization of Gaussian integers, Euclidean quadratic fields and Fermat's Last Theorem for the exponent p=3, to be covered in later chapters

Chapter 2 covers the standard basic material on Noetherian domains, Dedekind domains and factorial rings. These are applied to factoring methods for some cubic integers using Pollard's method and higher Fermat numbers

Chapter 3 covers the basics of binary quadratic forms from various points of view. It starts with material on equivalence, reduction and class numbers. Form class numbers and ideal class numbers are the compared, and an alternative proof of the finiteness of the ideal class number is given. The genus of forms is covered and the assigned values of generic characters via Jacobi symbols are described. These results are then applied to illustrate the equivalence of forms modulo a prime number.

Chapter 4 covers Diophantine approximation. Specifically, it studies the Thue-Siegel-Roth theorem, Schanuel's conjecture and gives an overview to the number theoretic constants of Gel'fond, Prouhet-Thue-Morse, Euler and Catalan. The chapter ends with some standard material on Minkowski's geometry of numbers.

Chapter 5 provides material on Bernoulli numbers and polynomials, Fourier series, the Euler-Maclaurin summation formula and an approximation of the Euler-Mascheroni constant. Then the famous Riemann-zeta function is briefly described, with a view towards the prime number theorem and Riemann's hypothesis.

Chapter 6 provides a standard introduction to the p-adic analysis, covering standard material on Hensel's Lemma, valuation theory and the representation of p-adic numbers as power series.

Chapter 7 first covers Dirichlet characters, their orthogonal identities, Dirichlet L-functions and the Generalized Riemann Hypothesis. These are used in the proof of Dirichlet's theorem on primes in arithmetic progression. The later part of the chapter covers Dirichlet densities, as well as the proof of the theorem on Dirichlet density of primes in arithmetic progressions.

Chapter 8 begins with a continuation of discussions from chapter 1, in particular, it begins by covering Lucas-Lehmer functions and how they are used in solving the generalized Ramanujan-Nagell equation as well as the Bachet equations. Fermat's last theorem for regular prime exponents is that discussed in some detail, including Kummer's proof of it. The later part of the chapter discusses the ABC conjecture and it's consequences, including the Thue-Siegel-Roth Theorem, Hall's Conjecture and the Granville-Langevin Conjecture.

Chapter 9 surveys elliptic curves over an arbitrary field, touching on torsion points, the Lutz-Nagell Theorem, Mazur's theorem and Siegel's theorem. Here, very few proofs are given, and the reader can gain more insight into the arithmetic theory of elliptic curves by doing some of the exercises included or by reading the references given. Some applications of elliptic curves are then presented, they include Lenstra's elliptic curve factoring method for odd natural numbers, his elliptic curve primality test, and the Menezes-Okamoto-Vanstone elliptic curve cryptosystem.

Chapter 10 gives a standard introduction to modular forms and in particular to elliptic modular functions. These concepts are used to describe the Shimura-Taniyama-Weil conjecture, which has now become the Modularity Theorem. It is then explained how this theorem implied Fermat's Last Theorem. The reader may gain a more thorough understanding of the later part of this chapter by using the references included, or by attempting some of the exercises.

3 Reviewer's Comments

This book offers a wide range of number theory topics for the student acquainted with the author's book 'Fundamental Number Theory with Applications'. The reader following this book will obtain a thorough overview of some very deep mathematics which is still in active research today. This book, whose contents are mostly explained clearly, offers a bridge between the basic material and the more advanced topics covered in research papers and monographs. Indeed, the reader will be tempted to explore some of the topics covered further from other more advanced texts.

While most material in this book are concise and come with proofs, the reader may want to supplement his reading by browsing other references, which the author has listed in relevant parts of the texts, as well as by doing the exercises the author has provided. This is especially true for chapters 9 and 10 where the author do not provide enough proofs (see the detailed description of chapters below). One very good point about this text is that solutions to odd-numbered exercises are provided at the back of

the book, so that the interested reader, should he want to, can be helped along quickly in better understanding the solution, and thus better understanding concepts in the text.

The use of biological sketches of relevant mathematicians sprinkled throughout the text is also a plus point. It breathes more life into the mathematics by talking about the people who did most of the important mathematics which became the basic and foundational material of today.

4 Reviewer's Recommendation

I readily recommend this book to advanced undergraduates and the beginning graduate student interested in advanced number theory. This book can also be read by the enthusiast who is well-acquainted with the author's previous book 'Fundamental Number Theory with Applications'.

The reviewer is a research scientist at the Centre of Strategic Infocomm Technologies (CSIT), Singapore.