DISCRETE MATHEMATICS AND ITS APPLICATIONS

Series Editor KENNETH H. ROSEN

FUNDAMENTAL NUMBER THEORY WITH APPLICATIONS

SECOND EDITION

RICHARD A. MOLLIN

Chapman & Hall/CRC
Taylor & Francis Group

DISCRETE MATHEMATICS AND ITS APPLICATIONS
Series Editor KENNETH H. ROSEN

FUNDAMENTAL NUMBER THEORY WITH APPLICATIONS

SECOND EDITION

RICHARD A. MOLLIN
University of Calgary
Alberta, Canada

Chapman & Hall/CRC
Taylor & Francis Group
Boca Raton London New York

Chapman & Hall/CRC is an imprint of the
Taylor & Francis Group, an **informa** business

Chapman & Hall/CRC
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed in the United States of America on acid-free paper
10 9 8 7 6 5 4 3 2 1

International Standard Book Number-13: 978-1-4200-6659-3 (Hardcover)

Library of Congress Cataloging-in-Publication Data

Mollin, Richard A., 1947-
Fundamental number theory with applications / Richard A. Mollin. -- 2nd ed.
p. cm. -- (Discrete mathematics and its applications ; 47)
Includes bibliographical references and index.
ISBN 978-1-4200-6659-3 (hardback : alk. paper)
1. Number theory. I. Title. II. Series.

QA241.M598 2008
512.7--dc22 2007050650

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Fundamental Number Theory with Applications

Second Edition

DISCRETE MATHEMATICS AND ITS APPLICATIONS

Series Editor
Kenneth H. Rosen, Ph.D.

Juergen Bierbrauer, Introduction to Coding Theory

Francine Blanchet-Sadri, Algorithmic Combinatorics on Partial Words

Kun-Mao Chao and Bang Ye Wu, Spanning Trees and Optimization Problems

Charalambos A. Charalambides, Enumerative Combinatorics

Henri Cohen, Gerhard Frey, et al., Handbook of Elliptic and Hyperelliptic Curve Cryptography

Charles J. Colbourn and Jeffrey H. Dinitz, Handbook of Combinatorial Designs, Second Edition

Martin Erickson and Anthony Vazzana, Introduction to Number Theory

Steven Furino, Ying Miao, and Jianxing Yin, Frames and Resolvable Designs: Uses, Constructions, and Existence

Randy Goldberg and Lance Riek, A Practical Handbook of Speech Coders

Jacob E. Goodman and Joseph O'Rourke, Handbook of Discrete and Computational Geometry, Second Edition

Jonathan L. Gross, Combinatorial Methods with Computer Applications

Jonathan L. Gross and Jay Yellen, Graph Theory and Its Applications, Second Edition

Jonathan L. Gross and Jay Yellen, Handbook of Graph Theory

Darrel R. Hankerson, Greg A. Harris, and Peter D. Johnson, Introduction to Information Theory and Data Compression, Second Edition

Daryl D. Harms, Miroslav Kraetzl, Charles J. Colbourn, and John S. Devitt, Network Reliability: Experiments with a Symbolic Algebra Environment

Leslie Hogben, Handbook of Linear Algebra

Derek F. Holt with Bettina Eick and Eamonn A. O'Brien, Handbook of Computational Group Theory

David M. Jackson and Terry I. Visentin, An Atlas of Smaller Maps in Orientable and Nonorientable Surfaces

Richard E. Klima, Neil P. Sigmon, and Ernest L. Stitzinger, Applications of Abstract Algebra with Maple™ and MATLAB®, Second Edition

Patrick Knupp and Kambiz Salari, Verification of Computer Codes in Computational Science and Engineering

Continued Titles

William Kocay and Donald L. Kreher, Graphs, Algorithms, and Optimization

Donald L. Kreher and Douglas R. Stinson, Combinatorial Algorithms: Generation Enumeration and Search

Charles C. Lindner and Christopher A. Rodgers, Design Theory

Hang T. Lau, A Java Library of Graph Algorithms and Optimization

Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, Handbook of Applied Cryptography

Richard A. Mollin, Algebraic Number Theory

Richard A. Mollin, Codes: The Guide to Secrecy from Ancient to Modern Times

Richard A. Mollin, Fundamental Number Theory with Applications, Second Edition

Richard A. Mollin, An Introduction to Cryptography, Second Edition

Richard A. Mollin, Quadratics

Richard A. Mollin, RSA and Public-Key Cryptography

Carlos J. Moreno and Samuel S. Wagstaff, Jr., Sums of Squares of Integers

Dingyi Pei, Authentication Codes and Combinatorial Designs

Kenneth H. Rosen, Handbook of Discrete and Combinatorial Mathematics

Douglas R. Shier and K.T. Wallenius, Applied Mathematical Modeling: A Multidisciplinary Approach

Jörn Steuding, Diophantine Analysis

Douglas R. Stinson, Cryptography: Theory and Practice, Third Edition

Roberto Togneri and Christopher J. deSilva, Fundamentals of Information Theory and Coding Design

W. D. Wallis, Introduction to Combinatorial Designs, Second Edition

Lawrence C. Washington, Elliptic Curves: Number Theory and Cryptography

Dedicated to the memory of Irving Kaplansky.

Preface

The second edition of the original introductory undergraduate text for a one-semester first course in number theory is redesigned to be more accessible and far reaching in its coverage from a truly "fundamental" perspective. This means that virtually all "advanced" material has been removed in favour of more topics at the elementary level, not included in the first edition. For instance, we have removed the algebraic number theory, elliptic curves, the (ideal-theoretic) continued fraction factoring algorithm, applications to quadratic orders, including ideals, the advanced material on quadratic polynomials, and applications to quadratics. There will be a second volume to be published that will have advanced material for a *second course* in number theory.

The background on arithmetic of the integers has been moved from the main text to Appendix A, and the discussion of complexity to Appendix B. More elementary material has been added, including partition theory and generating functions, combinatorial number theory, an expanded and more involved discussion of random number generation, more applications to cryptology, primality testing, and factoring. As well, there is an expanded coverage of Diophantine equations from a more elementary point of view, including a section for Legendre's Theorem on the equation $ax^2 + by^2 + cz^2 = 0$, and an expanded view of Bachet's equation $y^2 = x^3 + k$. Moreover, the coverage of sums of two, three, and four squares has been revised completely to concentrate on criteria for representation, and more on the total number of primitive representations, deleting the extensive coverage of the total number of imprimitive representations from the first edition. For sums of two squares, applications from continued fraction theory, not covered in the first edition, is discussed in detail. Sums of cubes is given a separate section, also not covered in the first edition. That rounds out Chapter Six on additivity.

The numbering system has been changed from the three-level approach (such as Theorem 1.2.3) to an easier, more standard two-level approach (such as Theorem 1.2). The use of footnotes has been curtailed in this edition. For instance, the mini-biographies are placed in highlighted boxes as sidebars to reduce distraction and impinging on text of footnote usage. Footnotes are employed only when no other mechanisms will work. Also, the Bibliography contains the page(s) where each entry is cited, another new inclusion, which helps the reader see the relevance of each such reference to the specific material in the text.

Other than the addition of Appendices A–B, as noted above, we retain the appendices from the first edition on primes and least primitive roots, indices, and the ABC conjecture, but have deleted the more specialized appendices on tables of special primes, Cunningham factorizations, pseudoprimes, Carmichael numbers, and values of some arithmetic functions. Also, although we also deleted the appendix from the first edition on the prime number theorem, we have included a section (§1.9) on distribution of primes that is more extensive, informative, and perhaps one of the few aspects of the main text that retains

a flavour of being "advanced," yet accessible via the method of presentation. Furthermore, we have added Appendix F on *Primes is in P*, to delineate the recently discovered unconditional deterministic polynomial-time algorithm for primality testing that is indeed "advanced". However, this is worth the inclusion, at the end of the text, for its impressive implications made available for the more adventurous reader, perhaps interested in going on to a second course in number theory.

The list of symbols is a single page of the most significant ones in use. The index has over thirteen hundred entries presented in such a fashion that there is maximum cross-referencing to ensure that the reader will find data with ease.

There are nearly 400 exercises in this edition, and there are nearly seventy mini-biographies. Also, the more challenging exercises are marked with the ☆ symbol. As with the first edition, solutions of the odd-numbered exercises are included at the end of the text, and a solutions manual for the even-numbered exercises is available to instructors who adopt the text for a course. As usual, the website below is designed for the reader to access any updates and the e-mail address below is available for any comments.

◆ **Acknowledgments** The author is grateful for the proofreading done by the following people, each of whom lent their own valuable time: John Burke (U.S.A.), Jacek Fabrykowski (U.S.A.), Bart Goddard (U.S.A.), and Thomas Zaplachinski (Canada), a former student, now cryptographer.

December 7, 2007

website: http://www.math.ucalgary.ca/~ramollin/

e-mail: ramollin@math.ucalgary.ca

Contents

Chapter 1

Arithmetic of the Integers

Philosophy is written in the great books which ever lies before our eyes — I mean the universe... This book is written in mathematical language and its characters are triangles, circles and other geometrical figures, without whose help...one wanders in vain through a dark labyrinth.

Galileo Galilei (1564–1642), Italian astronomer and physicist

In this introductory chapter, we discover the arithmetic underlying the integers and the tools to manipulate them. The reader should be familiar with the basic notation, symbols, set theory, and background in Appendix A.

1.1 Induction

An essential tool in number theory, which allows us in this section to prove the base representation theorem, is the following.

◆ Principle of Mathematical Induction — PMI

Suppose that $\mathcal{S} \subseteq \mathbb{N}$ and both (a) and (b) below hold.

(a) $1 \in \mathcal{S}$, and

(b) If $n > 1$ and $n - 1 \in \mathcal{S}$, then $n \in \mathcal{S}$.

Then $\mathcal{S} = \mathbb{N}$.

In other words, the Principle of Mathematical Induction says that any subset of the natural numbers that contains 1, and can be shown to contain $n > 1$ whenever it contains $n - 1$ must be $\mathbb{N}$. Part (a) is called the *induction step*, and the assumption that $n - 1 \in \mathcal{S}$ is called the *induction hypothesis*. First, one establishes the induction step, then assumes the induction hypothesis and

proves the conclusion, that $n \in \mathcal{S}$. Then we simply say that *by induction*, $n \in \mathcal{S}$ for all $n \in \mathbb{N}$. This principle is illustrated in the following two results.

Theorem 1.1 **A Summation Formula**

For any $n \in \mathbb{N}$,

$$\sum_{j=1}^{n} j = \frac{n(n+1)}{2}.$$

Proof. If $n = 1$, then $\sum_{j=1}^{n} j = 1 = n(n+1)/2$, and the induction step is secured. Assume that

$$\sum_{j=1}^{n-1} j = (n-1)n/2,$$

the induction hypothesis. Now consider

$$\sum_{j=1}^{n} j = n + \sum_{j=1}^{n-1} j = n + (n-1)n/2,$$

by the induction hypothesis. Hence,

$$\sum_{j=1}^{n} j = [2n + (n-1)n]/2 = (n^2 + n)/2 = n(n+1)/2,$$

as required. Hence, by induction, this must hold for all $n \in \mathbb{N}$. □

Theorem 1.2 **A Geometric Formula**

If $a, r \in \mathbb{R}$, $r \neq 1$, $n \in \mathbb{N}$, *then* $\sum_{j=0}^{n} ar^j = \frac{a(r^{n+1}-1)}{r-1}$.

Proof. If $n = 1$, then

$$\sum_{j=0}^{n} ar^j = a + ar = a(1+r) = a(1+r)(r-1)/(r-1) = a(r^2-1)/(r-1) =$$

$$a(r^{n+1}-1)/(r-1),$$

which is the induction step. By the induction hypothesis, we get

$$\sum_{j=0}^{n+1} ar^j = ar^{n+1} + \sum_{j=0}^{n} ar^j = ar^{n+1} + a(r^{n+1}-1)/(r-1) = a(r^{n+2}-1)/(r-1),$$

as required. □

The sum in Theorem 1.2 is called a *geometric sum* where a is the *initial term* and r is called the *ratio*.

Now we look at a classical problem involving rabbits as a vehicle for introducing a celebrated sequence that lends itself very well as an application of induction.

◆ The Rabbit Problem

Suppose that a male rabbit and a female rabbit have just been born. Assume that any given rabbit reaches sexual maturity after one month and that the gestation period for a rabbit is one month. Furthermore, once a female rabbit reaches sexual maturity, it will give birth every month to exactly one male and one female. Assuming that no rabbits die, how many male/female pairs are there after n months?

We will use the symbol F_n to denote the number of pairs of rabbits at month n, while M_n denotes the number of pairs of mature rabbits at month n, and I_n the number of immature rabbits at month n. Then

$$F_n = M_n + I_n.$$

Therefore, we have $F_1 = F_2 = 1$, and for any $n \geq 3$, $M_n = F_{n-1}$, and $I_n = M_{n-1}$, since every newborn pair at time n is the product of a mature pair at time $n-1$. Thus,

$$F_n = F_{n-1} + M_{n-1}.$$

Moreover, $M_{n-1} = F_{n-2}$. Thus, we have

$$F_n = F_{n-1} + F_{n-2}, \tag{1.1}$$

for any $n \geq 3$, which generates the *Fibonacci Sequence* — *see Biography 1.1.* (A research journal devoted entirely to the study of such numbers is the *Fibonacci Quarterly.*)

Biography 1.1 Fibonacci (ca.1180–1250) *was known as* Leonardo of Pisa, *the son of an Italian merchant named Bonaccio. He had an Arab scholar as his tutor while his father served as consul in North Africa. Thus, he was well educated in the mathematics known to the Arabs. Fibonacci's first and certainly his best-known book is* Liber Abaci *or* Book of the Abacus *first published in 1202, which was one of the means by which the Hindu-Arabic number system was transmitted into Europe. However, only the second edition, published in 1228, has survived. In this work, Fibonacci included work on geometry, the theory of proportion, and techniques for determining the roots of equations. Also included in his book was the rabbit problem described above.*
Perhaps his most prominent work, Liber Quadratorum *or* Book of Square Numbers, *published in 1225, contains some sophisticated contributions to number theory. Fibonacci dedicated this book to his patron, Holy Roman Emperor* Friedrich II *of Germany.*

We now prove a result, as an application of induction, attributed to Binet (see Biography 1.2 on the next page), that links the Fibonacci sequence with the famous *golden ratio*:

$$\mathfrak{g} = \frac{1+\sqrt{5}}{2}, \tag{1.2}$$

Theorem 1.3 **Binet's Formula**

F_n is the n-th Fibonacci number for any $n \in \mathbb{N}$, and

$$\mathfrak{g}' = \frac{1-\sqrt{5}}{2}$$

is the conjugate of the golden ratio, then

$$F_n = \frac{1}{\sqrt{5}}[\mathfrak{g}^n - \mathfrak{g}'^n] = \frac{\mathfrak{g}^n - \mathfrak{g}'^n}{\mathfrak{g} - \mathfrak{g}'},$$

Proof. We use induction. If $n = 1$, then

$$\frac{1}{\sqrt{5}}\left[\mathfrak{g}^n - \mathfrak{g}'^n\right] = \frac{1}{\sqrt{5}}\left[\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}\right] = \frac{\sqrt{5}}{\sqrt{5}} = 1 = F_n.$$

Assume that $F_n = \frac{1}{\sqrt{5}}[\mathfrak{g}^n - \mathfrak{g}'^n]$, which is the induction hypothesis, from which we have

$$F_{n+1} = F_n + F_{n-1} = \frac{1}{\sqrt{5}}\left[\mathfrak{g}^n - \mathfrak{g}'^n\right] + \frac{1}{\sqrt{5}}\left[\mathfrak{g}^{n-1} - \mathfrak{g}'^{n-1}\right],$$

and by factoring out appropriate powers, this is equal to

$$\frac{1}{\sqrt{5}}\left[\mathfrak{g}^{n-1}(1+\mathfrak{g}) - \mathfrak{g}'^{n-1}(1+\mathfrak{g}')\right].$$

By Exercise 1.1, $1 + \mathfrak{g} = \mathfrak{g}^2$. It may be similarly verified that $1 + \mathfrak{g}' = \mathfrak{g}'^2$. Hence,

$$F_{n+1} = \frac{1}{\sqrt{5}}[\mathfrak{g}^{n+1} - \mathfrak{g}'^{n+1}] = \frac{\mathfrak{g}^{n+1} - \mathfrak{g}'^{n+1}}{\mathfrak{g} - \mathfrak{g}'},$$

since $\mathfrak{g} - \mathfrak{g}' = \sqrt{5}$. □

The following result is a fascinating relationship between the golden ratio and Fibonacci numbers that is a consequence of the above.

Corollary 1.1 **Asymptotic Behaviour of Fibonacci Numbers**

If F_n denotes the n-th Fibonacci number and $\mathfrak{g}$ denotes the golden ratio, then

$$\lim_{n\to\infty} \frac{F_{n+1}}{F_n} = \mathfrak{g}.$$

Proof. By Theorem 1.3,

$$\lim_{n\to\infty}\frac{F_{n+1}}{F_n}=\lim_{n\to\infty}\frac{\mathfrak{g}^{n+1}-\mathfrak{g}'^{n+1}}{\mathfrak{g}^n-\mathfrak{g}'^n}=\mathfrak{g}\lim_{n\to\infty}\frac{\mathfrak{g}^n}{\mathfrak{g}^n-\mathfrak{g}'^n}-\mathfrak{g}'\lim_{n\to\infty}\frac{\mathfrak{g}'^n}{\mathfrak{g}^n-\mathfrak{g}'^n}=$$

$$\mathfrak{g}\lim_{n\to\infty}\frac{1}{\mathfrak{g}^n/\mathfrak{g}^n-\mathfrak{g}'^n/\mathfrak{g}^n}-\mathfrak{g}'\lim_{n\to\infty}\frac{1}{\mathfrak{g}^n/\mathfrak{g}'^n-\mathfrak{g}'^n/\mathfrak{g}'^n}=\mathfrak{g}\lim_{n\to\infty}1-0=\mathfrak{g},$$

since $\mathfrak{g}/\mathfrak{g}'>1$. □

Biography 1.2 Jacques Philippe Marie Binet (1786–1856) *was born on February 2 of 1786 in Rennes, Bretagne, France. After completing his education in 1806, he became a teacher at École Polytechnique in 1807. By 1816, after some other appointments, he became an inspector of studies at École Polytechnique, and by 1823 had been appointed to the astronomy chair at the Collège de France, which he held for more than 3 decades. For political reasons he was dismissed as inspector of studies on November 13, 1830. He is probably best known for his work on matrix theory, especially the rule for multiplying matrices, which was used later by Cayley, for instance, in extending the theory. He contributed to number theory as well, especially in the early 1840s. The paper that contains the formula with his name was published in 1843 — see* [6]. *However, as often happens with mathematical discoveries, it had already been discovered earlier. Indeed, de Moivre* [13] *had discovered it over a century earlier and in greater generality. Binet published in areas other than mathematics such as astronomy and physics, with a list of over 50 publications in total to his credit. He died on May 12, 1856 in Paris, France.*

The exercises at the end of this section contain numerous problems related to Fibonacci numbers and their generalizations. This includes links to the golden ratio and other values for the reader to get a better appreciation of these numerical sequences and their properties.

We now look at another interesting problem as an application of induction, a puzzle developed by François Édouard Anatole Lucas (see Biography 1.18 on page 63).

◆ Tower of Hanoi Problem

Assume that there are three vertical posts and $n \geq 1$ rings, all of different sizes, concentrically placed on one of the posts from largest on the bottom to smallest on the top. In other words, no larger ring is placed upon a smaller one. The object of the game is to move all rings from the given post to another post, subject to the following rules:

[1] Only one ring may be moved at a time.
[2] A ring may never be placed over a smaller ring.

We now use induction to show that the number of moves to transfer n rings from one post to another is $2^n - 1$.

Let $N(n)$ be the minimum number of moves required to do the above. First, we show that

$$N(n+1) = 2N(n) + 1.$$

To move the $(n+1)$-st (largest) ring to the destination post after $n \in \mathbb{N}$ rings have been moved there, we first move the rings to the unoccupied post, which requires $N(n)$ moves. Then we move the $(n+1)$-st ring to the destination post (one move). Finally, we move the original n rings back to the destination post, requiring another $N(n)$ moves for a total of $2N(n) + 1$ moves. Now, we use induction on n.

If $n = 1$, then $N(1) = 1$, and if $n = 2$, then $N(2) = 3 = 2^2 - 1$. Assume that the result holds for k such that $1 \leq k \leq n$. Hence,

$$N(n+1) = 2N(n) + 1 =$$

$$2(2^n - 1) + 1 = 2^{n+1} - 1.$$

Here is another tantalizing question that we can use the above to solve.

Ancient folklore tells us that monks in a temple tower were given 64 rings at the beginning of time. They were told to play the above game, and that the world would end when they were finished. Assume that the monks worked in shifts twenty-four hours per day, moving one ring per second without any errors. How long does the world last?

The answer is approximately 5,849,420,458 centuries!

Now we provide some further applications to induction by introducing the sequences related to Lucas, and their relationship with the Fibonacci sequence.

◆ The Lucas Sequence

The Lucas sequence for any $n \in \mathbb{N}$ is given by

$$L_n = \mathfrak{g}^n + \mathfrak{g}'^n, \tag{1.3}$$

where $\mathfrak{g}$ is the golden ratio introduced in (1.2) on page 4.

Now we show how the Lucas and Fibonacci sequences are related. Although this following result does not use induction directly, it does employ Theorem 1.3, which does use induction.

Theorem 1.4 **Lucas and Fibonacci Relationship**

For any $n \in \mathbb{N}$,

$$L_{n+1} = F_{n+2} + F_n.$$

Proof. By the definition of the Fibonacci numbers, $F_{n+2} + F_n = F_{n+1} + 2F_n$, and by Theorem 1.3,

$$F_{n+1} + 2F_n = \frac{\mathfrak{g}^{n+1} - \mathfrak{g}'^{n+1}}{\mathfrak{g} - \mathfrak{g}'} + 2\frac{\mathfrak{g}^n - \mathfrak{g}'^n}{\mathfrak{g} - \mathfrak{g}'} = \frac{\mathfrak{g}^{n+1} + 2\mathfrak{g}^n - \mathfrak{g}'^{n+1} - 2\mathfrak{g}'^n}{\mathfrak{g} - \mathfrak{g}'} =$$