

# Elementary Number Theory

Jie Xiao

Elementary Number Theory  
by Jie Xiao (Memorial University of Newfoundland)

Copyright © 2006, 2010 by International Press  
Somerville, Massachusetts, U.S.A.

All rights reserved. Individual readers of this publication, and non-profit libraries acting for them, are permitted to make fair use of the material, such as to copy a chapter for use in teaching or research. Permission is granted to quote brief passages from this publication in reviews, provided the customary acknowledgement of the source is given. Republication, systematic copying, or mass reproduction of any material in this publication is permitted only under license from International Press.

ISBN 978-1-57146-183-4

*Paperback reissue 2010.*  
*Previously published in 2006 under ISBN 978-1-57146-163-6 (clothbound).*

Typeset using the LaTeX system.  
[Printed in the USA on acid-free paper].

## Preface

Traditionally, elementary number theory is a branch of number theory dealing with the integers without use of techniques from other mathematical fields. With this objective in mind, and exercising as much control as possible over my own prejudices, I have sought to pare away all material that might be considered extraneous in a three hour per week, twelve week semester course in elementary number theory. This leads to my aim in writing this book: On the one hand, I must present in a well-motivated and natural sequence the basic ideas and results of elementary number theory. On the other hand, enough material is covered to provide a firm base on which to build for later studies in algebraic number theory and analytic number theory. The only background material required of the reader is a knowledge of some simple properties of the system of integers. Otherwise this concise book is self-contained.

The book begins with a few preliminaries on induction principles, followed by a quick review of division algorithm. The substance of the book starts in the second chapter, where, using divisors, the greatest (least) common divisor (multiple), the Euclidean algorithm and linear indeterminate equation are discussed. This foundation supports the subsequent chapters: prime numbers; congruences; congruent equations; and, finally, three additional topics (comprising cryptography, Diophantine equations and Gaussian integers). Placed at the end of each chapter are some exercises that illustrate the theory and provide practice in the techniques. Answers to all the even-numbered problems are given at the end of the book.

The above-mentioned material was used with groups of undergraduates in one-semester courses at Memorial University of Newfoundland. A brisk pace should make it possible to cover this little book in its entirety in one semester.

While writing this book I was encouraged by and benefited from a number of individuals. Here, I want to thank Hershy Kisilevsky at Concordia University as well as Herb Gaskill, Donald E. Rideout, Yiqiang Zhou and my students at Memorial University of Newfoundland for their helpful comments and suggestions. Meanwhile, I am very grateful to the referee for his invaluable review, but also to Shing-Tung Yau at Harvard University and Brian Bianchini and Lisa Lin at International Press for their practical advice. Last but not least, I wish to take this opportunity to acknowledge

my sense of indebtedness to my family for their considerable patience and understanding.

*Montreal & St. John's*  
*Summer 2002 & Fall 2005 – Spring 2006*

*Jie Xiao*

# Contents

Preface	iii
Chapter 1. Basics	1
1.1. Principles of Induction and Well-ordering	1
1.2. Equivalence of Principles	3
1.3. Division Algorithm	4
Exercises	5
Chapter 2. Divisibility	7
2.1. Divisors	7
2.2. The Greatest Common Divisor	7
2.3. The Euclidean Algorithm	9
2.4. Linear Indeterminate Equation	10
2.5. The Least Common Multiple	12
Exercises	13
Chapter 3. Primes	15
3.1. Number of Primes	15
3.2. The Fundamental Theorem of Arithmetic	16
3.3. The Bracket Function	19
3.4. Mersenne, Fermat, and Perfect Numbers	21
Exercises	23
Chapter 4. Congruences	25
4.1. Simple Properties	25
4.2. Residue Systems	27
4.3. Euler's and Fermat's Little Theorems	31
4.4. Orders and Indices	33
Exercises	37
Chapter 5. Congruent Equations	39
5.1. Linear Congruences and CRT	39
5.2. Lagrange's and Wilson's Theorems	44
5.3. Quadratic Residues	47
Exercises	54
Chapter 6. Three Additional Topics	57
6.1. Cryptography by Caesar and RSA	57

6.2. Diophantine Equations $x^n + y^n = z^n$ , $n \geq 2$	61
6.3. Gaussian Integers	65
Exercises	70
Solutions to Even-numbered Exercises	73
1. Basics	73
2. Divisibility	74
3. Primes	75
4. Congruences	76
5. Congruent Equations	78
6. Three Additional Topics	79
Bibliography	81
Index	83