Review of the book

*"An Introduction to Number Theory with Cryptography"*

by James S. Kraft and Lawrence C. Washington

CRC Press, Taylor & Francis Group, 2014

ISBN: 978-1-4822-1441-3

S. V. Nagaraj

2014-09-20

## 1 Summary of the review

Number theory is a fascinating branch of mathematics. This review is about an introductory book on number theory and cryptography. The book offers an introduction to number theory along with its interesting applications in cryptography. The book has eighteen chapters.

## 2 Summary of the book

The book is an introductory text that contains basics of number theory and some of its cryptographic applications. It is made up of eighteen chapters.

Chapter 0 (Introduction) offers a brief overview of Diophantine equations; modular arithmetic; primes and their distribution; and cryptography.

Chapter 1 (Divisibility) offers insight into the process of division; the Eratosthenes sieve; the greatest common divisor; and the Euclidean algorithm and its extended version.

Chapter 2 (Unique Factorization) looks at the fundamental theorem of arithmetic and the concept of unique factorization.

Chapter 3 (Applications of Unique Factorization) studies proofs of irrationality; the rational root theorem; Pythogorean triples; differences of squares; prime factorization of factorials; and the Riemann zeta function.

Chapter 4 (Congruences) describes modular exponentiation; tests for divisibility; linear congruences; the Chinese remainder theorem; theorems of Fermat, Euler and Wilson; and the arrangement of queens on a chess board.

Chapter 5 (Cryptographic Applications) explains shift and affine functions; secret sharing; and the RSA cryptosystem.

Chapter 6 (Polynomial Congruences) provides a brief overview of polynomials modulo primes; solutions modulo prime powers; and composite moduli.

Chapter 7 (Order and Primitive Roots) brings in the concept of orders of elements; primitive roots; decimals; card shuffling; the discrete log problem; and the existence of primitive roots.

Chapter 8 (More Cryptographic Applications) familiarizes the reader with Diffie-Hellman key exchange;

coin flipping over the telephone; mental poker; the ElGamal cryptosystem; and digital signatures.

Chapter 9 (Quadratic Reciprocity) discusses squares and square roots modulo primes; quadratic equations; the Jacobi symbol; and the proof of quadratic reciprocity.

Chapter 10 (Primality and Factorization) highlights trial division and Fermat factorization; primality testing; factorization; and revisits coin flipping over the telephone.

Chapter 11 (Geometry of Numbers) looks at Minkowski's theorem; sums of two squares; sums of four squares; and the Pell equation.

Chapter 12 (Arithmetic Functions) describes perfect numbers and multiplicative functions.

Chapter 13 (Continued Fractions) discusses rational approximations; rational numbers; periodic continued fractions; square roots of integers; and irrational numbers.

Chapter 14 (Gaussian Integers) studies complex arithmetic; Gaussian irreducibles; the division algorithm; unique factorization; and applications of Gaussian integers.

Chapter 15 (Algebraic Integers) describes quadratic fields and algebraic integers; units; and non-unique factorization.

Chapter 16 (Analytic Methods) demonstrates that the sum of reciprocals of primes diverges. It also discusses Bertrand's postulate and Chebyshev's approximate prime number theorem.

Chapter 17 (Epilogue: Fermat's Last Theorem) is the final chapter of the book. It provides an introduction to the proof techniques that were used in solving Fermat's last theorem.

Supplementary topics have also been included at the end of the book. These topics are geometric series; mathematical induction; Pascal's triangle and the binomial theorem; and Fibonacci numbers. Answers and hints are also provided for odd-numbered exercises. The book includes a short index. Many chapters of the book include exercises; projects; computer explorations; and answers for checking the reader's understanding of the subject matter of the book.

## 3 What is the book like (style)?

The book offers a basic introduction to number theory and some of its applications to cryptography. The book is an introductory textbook. The supplementary material in the book is quite helpful for self-learning and pedagogy. The book is well written and highly readable. This book is well suited for beginners and undergrads. The problems and exercises at the end of chapters will help the readers to test their comprehension.

## 4 Would you recommend this book?

This book offers an excellent introduction to number theory and some of its applications to cryptography. It will be helpful for novices and students. I recommend this book as a useful introductory text on number theory and its cryptographic applications.

*The reviewer is a freelancer in Chennai, India*