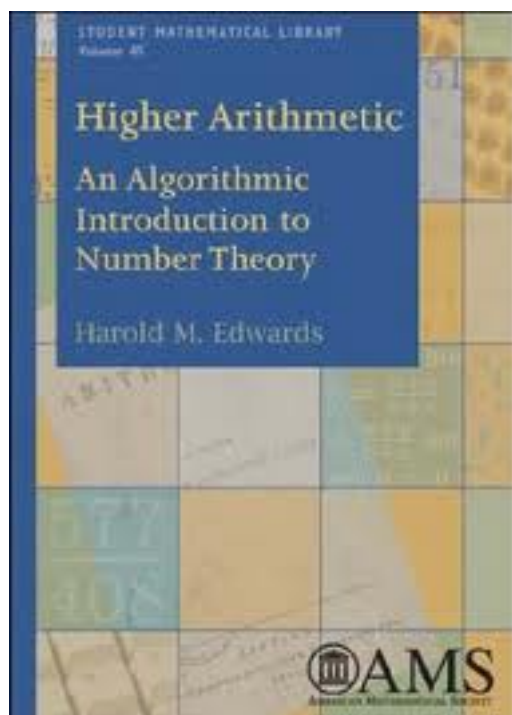


Higher Arithmetic



[Higher Arithmetic_下载链接1](#)

著者:Harold M. Edwards

出版者:American Mathematical Society

出版时间:2008-3-26

装帧:Paperback

isbn:9780821844397

Although number theorists have sometimes shunned and even disparaged computation in the past, today's applications of number theory to cryptography and computer security demand vast arithmetical computations. These demands have shifted the focus of studies in number theory and have changed attitudes toward computation itself.

The important new applications have attracted a great many students to number theory, but the best reason for studying the subject remains what it was when Gauss published his classic *Disquisitiones Arithmeticae* in 1801: Number theory is the equal of

Euclidean geometry—some would say it is superior to Euclidean geometry—as a model of pure, logical, deductive thinking. An arithmetical computation, after all, is the purest form of deductive argument.

Higher Arithmetic explains number theory in a way that gives deductive reasoning, including algorithms and computations, the central role. Hands-on experience with the application of algorithms to computational examples enables students to master the fundamental ideas of basic number theory. This is a worthwhile goal for any student of mathematics and an essential one for students interested in the modern applications of number theory.

作者介绍:

Harold M. Edwards is Emeritus Professor of Mathematics at New York University. His previous books are Advanced Calculus (1969, 1980, 1993), Riemann's Zeta Function (1974, 2001), Fermat's Last Theorem (1977), Galois Theory (1984), Divisor Theory (1990), Linear Algebra (1995), and Essays in Constructive Mathematics (2005). For his masterly mathematical exposition he was awarded a Steele Prize as well as a Whiteman Prize by the American Mathematical Society.

目录: Cover 1

Title 4

Copyright 5

Contents 6

Preface 10

Chapter 1. Numbers 14

Chapter 2. The Problem [omitted] 20

Chapter 3. Congruences 24

Chapter 4. Double Congruences and the Euclidean Algorithm 30

Chapter 5. The Augmented Euclidean Algorithm 36

Chapter 6. Simultaneous Congruences 42

Chapter 7. The Fundamental Theorem of Arithmetic 46

Chapter 8. Exponentiation and Orders 50

Chapter 9. Euler's ϕ -Function 56

Chapter 10. Finding the Order of $a \bmod c$ 58

Chapter 11. Primality Testing 64

Chapter 12. The RSA Cipher System 70

Chapter 13. Primitive Roots $\bmod p$ 74

Chapter 14. Polynomials 80

Chapter 15. Tables of Indices $\bmod p$ 84

Chapter 16. Brahmagupta's Formula and Hypernumbers 90

Chapter 17. Modules of Hypernumbers 94

Chapter 18. A Canonical Form for Modules of Hypernumbers 100

Chapter 19. Solution of [omitted] 106

Chapter 20. Proof of the Theorem of Chapter 19 112

Chapter 21. Euler's Remarkable Discovery 126

Chapter 22. Stable Modules 132

Chapter 23. Equivalence of Modules 136

Chapter 24. Signatures of Equivalence Classes 142

Chapter 25. The Main Theorem 148

Chapter 26. Modules That Become Principal When Squared 150

Chapter 27. The Possible Signatures for Certain Values of A 156

Chapter 28. The Law of Quadratic Reciprocity 162
Chapter 29. Proof of the Main Theorem 166
Chapter 30. The Theory of Binary Quadratic Forms 168
Chapter 31. Composition of Binary Quadratic Forms 176
Appendix. Cycles of Stable Modules 182
Answers to Exercises 192
Bibliography 220
Index 222
A 222
B 222
C 222
D 222
E 222
F 222
G 223
H 223
I 223
J 223
K 223
L 223
M 223
N 223
O 223
P 223
Q 223
R 223
S 223
T 223
Back Cover 226
• • • • • ([收起](#))

[Higher Arithmetic 下载链接1](#)

标签

算法化

科普

数论

Edwards

评论

[Higher Arithmetic_下载链接1](#)

书评

[Higher Arithmetic_下载链接1](#)