

## Contents

Preface	page ix
Solving the Pell equation HENDRIK W. LENSTRA, JR.	1
Basic algorithms in number theory JOE BUHLER AND STAN WAGON	25
Smooth numbers and the quadratic sieve CARL POMERANCE	69
The number field sieve PETER STEVENHAGEN	83
Four primality testing algorithms RENÉ SCHOOF	101
Lattices HENDRIK W. LENSTRA, JR.	127
Elliptic curves BJORN POONEN	183
The arithmetic of number rings PETER STEVENHAGEN	209
Smooth numbers: computational number theory and beyond ANDREW GRANVILLE	267
Fast multiplication and its applications DANIEL J. BERNSTEIN	325
Elementary thoughts on discrete logarithms CARL POMERANCE	385
The impact of the number field sieve on the discrete logarithm problem in finite fields OLIVER SCHIROKAUER	397
Reducing lattice bases to find small-height values of univariate polynomials DANIEL J. BERNSTEIN	421
Computing Arakelov class groups RENÉ SCHOOF	447

Computational class field theory	497
HENRI COHEN AND PETER STEVENHAGEN	
Protecting communications against forgery	535
DANIEL J. BERNSTEIN	
Algorithmic theory of zeta functions over finite fields	551
DAQING WAN	
Counting points on varieties over finite fields of small characteristic	579
ALAN G. B. LAUDER AND DAQING WAN	
Congruent number problems and their variants	613
JAAP TOP AND NORIKO YUI	
An introduction to computing modular forms using modular symbols	641
WILLIAM A. STEIN	