

Contents

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

Cambridge University Press

978-0-521-80854-5 - Algorithmic Number Theory: Lattices, Number Fields, Curves and
Cryptography

Edited by J. P. Buhler and P. Stevenhagen

Table of Contents

[More information](#)

viii

CONTENTS

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	