

Primality Testing and Integer Factorization in Public-Key Cryptography

Second Edition

by

Song Y. Yan

*Harvard University
and
Massachusetts Institute of Technology
USA*



Springer

Author:

Dr. Song Y. Yan
Visiting Professor
Department of Mathematics
Harvard University
One Oxford Street
Cambridge, MA 02138-2901
syang@math.harvard.edu

and

Department of Mathematics
Massachusetts Institute of Technology
77 Massachusetts Avenue
Cambridge, MA 02139-4307
syang@math.mit.edu

Library of Congress Control Number: 2008935407

ISBN-13: 978-0-387-77267-7

e-ISBN-13: 978-0-387-77268-4

© 2009 Springer Science+Business Media, LLC.

All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer Science+Business Media, LLC, 233 Spring Street, New York, NY 10013, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden. The use in this publication of trade names, trademarks, service marks and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

Printed on acid-free paper

springer.com



In Memory of Prof Shiing-Shen Chern (1911–2004)

Founding Director, Mathematical Sciences Research Institute, Berkeley

Table of Contents

Preface to the Second Edition	ix
Preface to the First Edition	xi
1. Number-Theoretic Preliminaries	1
1.1 Problems in Number Theory	1
1.2 Groups, Rings and Fields	13
1.3 Divisibility Properties	23
1.4 Euclid's Algorithm and Continued Fractions	34
1.5 Arithmetic Functions $\sigma(n), \tau(n), \phi(n), \lambda(n), \mu(n)$	50
1.6 Linear Congruences	63
1.7 Quadratic Congruences	85
1.8 Primitive Roots and Power Residues	103
1.9 Arithmetic of Elliptic Curves	113
1.10 Chapter Notes and Further Reading	124
2. Primality Testing and Prime Generation	127
2.1 Computing with Numbers and Curves	127
2.2 Riemann ζ and Dirichlet L Functions	139
2.3 Rigorous Primality Tests	149
2.4 Compositeness and Pseudoprimalty Tests	157
2.5 Lucas Pseudoprimalty Test	168
2.6 Elliptic Curve Primality Tests	172
2.7 Superpolynomial-Time Tests	177
2.8 Polynomial-Time Tests	182
2.9 Comparison of General Purpose Primality Tests	188
2.10 Primality Tests for Special Numbers	192
2.11 Prime Number Generation	201
2.12 Chapter Notes and Further Reading	207
3. Integer Factorization and Discrete Logarithms	209
3.1 Introduction	209
3.2 Simple Factoring Methods	212
3.3 Elliptic Curve Method (ECM)	221

3.4	General Factoring Congruence	226
3.5	Continued FRAction Method (CFRAC)	230
3.6	Quadratic Sieve (QS)	234
3.7	Number Field Sieve (NFS).....	239
3.8	Quantum Factoring Algorithm	251
3.9	Discrete Logarithms	257
3.10	k th Roots	270
3.11	Elliptic Curve Discrete Logarithms	278
3.12	Chapter Notes and Further Reading	285
4.	Number-Theoretic Cryptography	287
4.1	Public-Key Cryptography	287
4.2	RSA Cryptosystem	292
4.3	Security and Cryptanalysis of RSA	301
4.4	Rabin Cryptography	314
4.5	Quadratic Residuosity Cryptography	320
4.6	Discrete Logarithm Cryptography	326
4.7	Elliptic Curve Cryptography	331
4.8	Zero-Knowledge Techniques.....	338
4.9	Deniable Authentication.....	341
4.10	Non-Factoring Based Cryptography	346
4.11	Chapter Notes and Further Reading	351
	Bibliography.....	353
	Index.....	367
	About the Author	373