

Primality and Cryptography

Evangelos Kranakis
*Universiteit van Amsterdam
Fakultaire Vakgroep Informatica
Amsterdam, Netherlands*

AND

*Yale University
Department of Computer Science
New Haven, USA*



B. G. TEUBNER
Stuttgart



JOHN WILEY & SONS
Chichester · New York · Brisbane · Toronto · Singapore

in

rik.

lar Algorithms
erification

TABLE OF CONTENTS

xiii

PROLOGUE

vii

TABLE OF CONTENTS

xiii

1	NUMBER THEORY	1
1.1	Introduction	1
1.2	The Homomorphism Theorem	2
1.3	Fibonacci Numbers	3
1.4	Congruences	4
1.5	The Chinese Remainder Theorem	7
1.6	Modular Exponentiation	10
1.7	Primitive Roots	11
1.8	Artin's Conjecture	14
1.9	The Carmichael Function	15
1.10	The Legendre Symbol	16
1.11	The Legendre-Jacobi Symbol	17
1.12	Computing Square Roots	21
1.13	Indices	24
1.14	Computing Indices	25
1.15	The Prime Number Theorem	28
1.16	Continued Fractions	31
1.17	Bibliographical Remarks	37
2	PRIMALITY TESTS	39
2.1	Introduction	39
2.2	The Sieve of Eratosthenes	40
2.3	Wilson's Test	41
2.4	Lucas's Test	42
2.5	Sum of Two Squares Test	43
2.6	Pratt's Test	46
2.7	Proth's Test	49
2.8	Pepin's Test	51
2.9	Lucas-Lehmer Test	51
2.10	Extended Riemann Hypothesis	55
2.11	Solovay-Strassen Deterministic Test	56
2.12	A Variant of the Solovay-Strassen Test	58
2.13	Miller's Deterministic Test	59
2.14	An Improvement of Miller's Test	62
2.15	Selfridge-Weinberger Test	63

2.16	Probabilistic (Monte Carlo) Primality Tests	65
2.17	Solovay-Strassen Test	66
2.18	Rabin's Test	68
2.19	Rumey-Adleman Test	73
2.20	Bibliographical Remarks	78
3	PROBABILITY THEORY	80
3.1	Introduction	80
3.2	Basic Notions	80
3.3	Random Variables	82
3.4	The Binomial Distribution	88
3.5	Chebyshev's Law of Large Numbers	90
3.6	Bernshtein's Law of Large Numbers	91
3.7	The Monte Carlo Method	94
3.8	Bibliographical Remarks	96
4	PSEUDORANDOM GENERATORS	98
4.1	Introduction	98
4.2	The Linear Congruence Generator	99
4.3	The $(1/p)$ - Generator	104
4.4	Quadratic Residues in Cryptography	108
4.5	Factoring and Quadratic Residues	110
4.6	Periodicity of Quadratic Residues	111
4.7	The Circuit as a Model of Computation	114
4.8	The Quadratic Residue Generator	117
4.9	The Quadratic Residuosity Assumption	124
4.10	The Index Generator	127
4.11	The Discrete Logarithm Assumption	135
4.12	Bibliographical Remarks	136
5	PUBLIC KEY CRYPTOSYSTEMS	138
5.1	Introduction	138
5.2	The Setup of a Nonpublic Key Cryptosystem	139
5.3	The Setup of a Public Key Cryptosystem	140
5.4	The RSA System	142
5.5	RSA Bits	145
5.6	The Rabin System	151
5.7	Rabin Bits	153
5.8	The Merkle - Hellman System	155

5.9	Security of the Merkle - Hellman System (Outline)	157
5.10	The Quadratic Residue System	160
5.11	Bibliographical Remarks	168

6 TOWARDS A GENERAL THEORY 170

6.1	Introduction	170
6.2	Security Tests	171
6.3	Pseudorandom Functions	178
6.4	Xoring	180
6.5	Proof of the XOR Lemma	186
6.6	Two Applications of the XOR Lemma	199
6.7	(One to One) One Way Functions	201
6.8	Random Polynomial and Deterministic Time	206
6.9	Bibliographical Remarks	208

REFERENCES 210

FREQUENTLY USED NOTATION 223

INDEX 228