

M. R. Schroeder

---

# Number Theory in Science and Communication

With Applications in Cryptography,  
Physics, Digital Information, Computing,  
and Self-Similarity

Fourth Edition  
With 99 Figures

 Springer

# Contents

---

## Part I. A Few Fundamentals

---

<b>1. Introduction</b> .....	1
The Family of Numbers .....	4
1.1 Fibonacci, Continued Fractions and the Golden Ratio .....	7
1.2 Fermat, Primes and Cyclotomy .....	9
1.3 Euler, Totients and Cryptography .....	11
1.4 Gauss, Congruences and Diffraction .....	13
1.5 Galois, Fields and Codes .....	14
<b>2. The Natural Numbers</b> .....	19
2.1 The Fundamental Theorem .....	19
2.2 The Least Common Multiple .....	20
2.3 Planetary “Gears” .....	21
2.4 The Greatest Common Divisor .....	21
2.5 Human Pitch Perception .....	23
2.6 Octaves, Temperament, Kilos and Decibels .....	24
2.7 Coprimes .....	26
2.8 Euclid’s Algorithm .....	26
2.9 The Decimal System Decimated .....	27
<b>3. Primes</b> .....	28
3.1 How Many Primes are There? .....	28
3.2 The Sieve of Eratosthenes .....	29
3.3 A Chinese Theorem in Error .....	30
3.4 A Formula for Primes .....	31
3.5 Mersenne Primes .....	32
3.6 Repunits .....	36
3.7 Perfect Numbers .....	37
3.8 Fermat Primes .....	38
3.9 Gauss and the Impossible Heptagon .....	39
<b>4. The Prime Distribution</b> .....	41
4.1 A Probabilistic Argument .....	41
4.2 The Prime-Counting Function $\pi(x)$ .....	43

4.3	David Hilbert and Large Nuclei .....	47
4.4	Coprime Probabilities .....	48
4.5	Primes in Progressions .....	51
4.6	Primeless Expanses .....	53
4.7	Squarefree and Coprime Integers .....	54
4.8	Twin Primes .....	54
4.9	Prime Triplets .....	56
4.10	Prime Quadruplets and Quintuplets .....	57
4.11	Primes at Any Distance .....	58
4.12	Spacing Distribution Between Adjacent Primes .....	61
4.13	Goldbach's Conjecture .....	61
4.14	Sum of Three Primes .....	63

---

## Part II. Some Simple Applications

---

5.	<b>Fractions: Continued, Egyptian and Farey</b> .....	65
5.1	A Neglected Subject .....	65
5.2	Relations with Measure Theory .....	69
5.3	Periodic Continued Fractions .....	70
5.4	Electrical Networks and Squared Squares .....	73
5.5	Fibonacci Numbers and the Golden Ratio .....	74
5.6	Fibonacci, Rabbits and Computers .....	78
5.7	Fibonacci and Divisibility .....	81
5.8	Generalized Fibonacci and Lucas Numbers .....	81
5.9	Egyptian Fractions, Inheritance and Some Unsolved Problems .....	85
5.10	Farey Fractions .....	86
5.10.1	Farey Trees .....	88
5.10.2	Locked Pallas .....	92
5.11	Fibonacci and the Problem of Bank Deposits .....	93
5.12	Error-Free Computing .....	94

---

## Part III. Congruences and the Like

---

6.	<b>Linear Congruences</b> .....	99
6.1	Residues .....	99
6.2	Some Simple Fields .....	102
6.3	Powers and Congruences .....	103
7.	<b>Diophantine Equations</b> .....	106
7.1	Relation with Congruences .....	106
7.2	A Gaussian Trick .....	107
7.3	Nonlinear Diophantine Equations .....	109

7.4	Triangular Numbers .....	110
7.5	Pythagorean Numbers .....	112
7.6	Exponential Diophantine Equations .....	113
7.7	Fermat's Last "Theorem" .....	113
7.8	The Demise of a Conjecture by Euler .....	115
7.9	A Nonlinear Diophantine Equation in Physics and the Geometry of Numbers .....	116
7.10	Normal-Mode Degeneracy in Room Acoustics (A Number-Theoretic Application) .....	120
7.11	Waring's Problem .....	121
<b>8.</b>	<b>The Theorems of Fermat, Wilson and Euler .....</b>	<b>122</b>
8.1	Fermat's Theorem .....	122
8.2	Wilson's Theorem .....	123
8.3	Euler's Theorem .....	124
8.4	The Impossible Star of David .....	125
8.5	Dirichlet and Linear Progression .....	127
<hr/>		
<b>Part IV. Cryptography and Divisors</b>		
<hr/>		
<b>9.</b>	<b>Euler Trap Doors and Public-Key Encryption .....</b>	<b>129</b>
9.1	A Numerical Trap Door .....	131
9.2	Digital Encryption .....	132
9.3	Public-Key Encryption .....	133
9.4	A Simple Example .....	135
9.5	Repeated Encryption .....	136
9.6	Summary and Encryption Requirements .....	137
<b>10.</b>	<b>The Divisor Functions .....</b>	<b>139</b>
10.1	The Number of Divisors .....	139
10.2	The Average of the Divisor Function .....	142
10.3	The Geometric Mean of the Divisors .....	142
10.4	The Summatory Function of the Divisor Function .....	143
10.5	The Generalized Divisor Functions .....	143
10.6	The Average Value of Euler's Function .....	144
<b>11.</b>	<b>The Prime Divisor Functions .....</b>	<b>146</b>
11.1	The Number of Different Prime Divisors .....	146
11.2	The Distribution of $\omega(n)$ .....	150
11.3	The Number of Prime Divisors .....	151
11.4	The Harmonic Mean of $\Omega(n)$ .....	154
11.5	Medians and Percentiles of $\Omega(n)$ .....	156
11.6	Implications for Public-Key Encryption .....	157

<b>12. Certified Signatures</b> .....	158
12.1 A Story of Creative Financing .....	158
12.2 Certified Signature for Public-Key Encryption .....	158
<b>13. Primitive Roots</b> .....	160
13.1 Orders .....	160
13.2 Periods of Decimal and Binary Fractions .....	163
13.3 A Primitive Proof of Wilson's Theorem .....	166
13.4 The Index – A Number-Theoretic Logarithm .....	166
13.5 Solution of Exponential Congruences .....	167
13.6 What is the Order $T_m$ of an Integer $m$ Modulo a Prime $p$ ? ..	169
13.7 Index “Encryption” .....	170
13.8 A Fourier Property of Primitive Roots and Concert Hall Acoustics .....	170
13.9 More Spacious-Sounding Sound .....	172
13.10 Galois Arrays for X-Ray Astronomy .....	174
13.11 A Negative Property of the Fermat Primes .....	175
<b>14. Knapsack Encryption</b> .....	177
14.1 An Easy Knapsack .....	177
14.2 A Hard Knapsack .....	178

---

## Part V. Residues and Diffraction

---

<b>15. Quadratic Residues</b> .....	181
15.1 Quadratic Congruences .....	181
15.2 Euler's Criterion .....	182
15.3 The Legendre Symbol .....	183
15.4 A Fourier Property of Legendre Sequences .....	185
15.5 Gauss Sums .....	185
15.6 Pretty Diffraction .....	187
15.7 Quadratic Reciprocity .....	187
15.8 A Fourier Property of Quadratic-Residue Sequences .....	188
15.9 Spread Spectrum Communication .....	190
15.10 Generalized Legendre Sequences Obtained Through Complexification of the Euler Criterion .....	191

---

## Part VI. Chinese and Other Fast Algorithms

---

<b>16. The Chinese Remainder Theorem and Simultaneous Congruences</b> .....	194
16.1 Simultaneous Congruences .....	194
16.2 The Sino-Representation: A Chinese Number System .....	195

16.3	Applications of the Sino-Representation .....	196
16.4	Discrete Fourier Transformation in Sino .....	198
16.5	A Sino-Optical Fourier Transformer .....	199
16.6	Generalized Sino-Representation .....	200
16.7	Fast Prime-Length Fourier Transform .....	201
<b>17.</b>	<b>Fast Transformation and Kronecker Products .....</b>	<b>203</b>
17.1	A Fast Hadamard Transform .....	203
17.2	The Basic Principle of the Fast Fourier Transforms .....	206
<b>18.</b>	<b>Quadratic Congruences .....</b>	<b>207</b>
18.1	Application of the Chinese Remainder Theorem (CRT) .....	207

## **Part VII. Pseudoprimes, Möbius Transform, and Partitions**

<b>19.</b>	<b>Pseudoprimes, Poker and Remote Coin Tossing .....</b>	<b>209</b>
19.1	Pulling Roots to Ferret Out Composites .....	209
19.2	Factors from a Square Root .....	210
19.3	Coin Tossing by Telephone .....	212
19.4	Absolute and Strong Pseudoprimes .....	214
19.5	Fermat and Strong Pseudoprimes .....	216
19.6	Deterministic Primality Testing .....	216
19.7	A Very Simple Factoring Algorithm .....	218
19.8	Factoring with Elliptic Curves .....	218
19.9	Quantum Factoring .....	219
<b>20.</b>	<b>The Möbius Function and the Möbius Transform .....</b>	<b>220</b>
20.1	The Möbius Transform and Its Inverse .....	220
20.2	Proof of the Inversion Formula .....	222
20.3	Second Inversion Formula .....	223
20.4	Third Inversion Formula .....	223
20.5	Fourth Inversion Formula .....	224
20.6	Riemann's Hypothesis and the Disproof of the Mertens Conjecture .....	224
20.7	Dirichlet Series and the Möbius Function .....	225
<b>21.</b>	<b>Generating Functions and Partitions .....</b>	<b>228</b>
21.1	Generating Functions .....	228
21.2	Partitions of Integers .....	230
21.3	Generating Functions of Partitions .....	231
21.4	Restricted Partitions .....	232

---

**Part VIII. Cyclotomy and Polynomials**


---

<b>22. Cyclotomic Polynomials</b>	236
22.1 How to Divide a Circle into Equal Parts	236
22.2 Gauss's Great Insight	239
22.3 Factoring in Different Fields	243
22.4 Cyclotomy in the Complex Plane	243
22.5 How to Divide a Circle with Compass and Straightedge	244
22.5.1 Rational Factors of $z^N - 1$	246
22.6 An Alternative Rational Factorization	247
22.7 Relation Between Rational Factors and Complex Roots	248
22.8 How to Calculate with Cyclotomic Polynomials	249
<b>23. Linear Systems and Polynomials</b>	251
23.1 Impulse Responses	251
23.2 Time-Discrete Systems and the $z$ Transform	252
23.3 Discrete Convolution	252
23.4 Cyclotomic Polynomials and $z$ Transform	253
<b>24. Polynomial Theory</b>	254
24.1 Some Basic Facts of Polynomial Life	254
24.2 Polynomial Residues	255
24.3 Chinese Remainders for Polynomials	256
24.4 Euclid's Algorithm for Polynomials	257

---

**Part IX. Galois Fields and More Applications**


---

<b>25. Galois Fields</b>	260
25.1 Prime Order	260
25.2 Prime Power Order	260
25.3 Generation of $GF(2^4)$	262
25.4 How Many Primitive Elements?	264
25.5 Recursive Relations	264
25.6 How to Calculate in $GF(p^m)$	266
25.7 Zech Logarithm, Doppler Radar and Optimum Ambiguity Functions	267
25.8 A Unique Phase-Array Based on the Zech Logarithm	270
25.9 Spread-Spectrum Communication and Zech Logarithms	272
<b>26. Spectral Properties of Galois Sequences</b>	273
26.1 Circular Correlation	273
26.2 Application to Error-Correcting Codes and Speech Recognition	275

26.3	Application to Precision Measurements . . . . .	277
26.4	Concert Hall Measurements . . . . .	278
26.5	The Fourth Effect of General Relativity . . . . .	279
26.6	Toward Better Concert Hall Acoustics . . . . .	280
26.7	Higher-Dimensional Diffusors . . . . .	285
26.8	Active Array Applications . . . . .	286
<b>27.</b>	<b>Random Number Generators . . . . .</b>	<b>287</b>
27.1	Pseudorandom Galois Sequences . . . . .	288
27.2	Randomness from Congruences . . . . .	289
27.3	"Continuous" Distributions . . . . .	290
27.4	Four Ways to Generate a Gaussian Variable . . . . .	291
27.5	Pseudorandom Sequences in Cryptography . . . . .	292
<b>28.</b>	<b>Waveforms and Radiation Patterns . . . . .</b>	<b>293</b>
28.1	Special Phases . . . . .	294
28.2	The Rudin-Shapiro Polynomials . . . . .	296
28.3	Gauss Sums and Peak Factors . . . . .	297
28.4	Galois Sequences and the Smallest Peak Factors . . . . .	299
28.5	Minimum Redundancy Antennas . . . . .	301
28.6	Golomb Rulers . . . . .	303
<b>29.</b>	<b>Number Theory, Randomness and "Art" . . . . .</b>	<b>305</b>
29.1	Number Theory and Graphic Design . . . . .	305
29.2	The Primes of Gauss and Eisenstein . . . . .	307
29.3	Galois Fields and Impossible Necklaces . . . . .	308
29.4	"Baroque" Integers . . . . .	312

---

## Part X. Self-Similarity, Fractals and Art

---

<b>30.</b>	<b>Self-Similarity, Fractals, Deterministic Chaos and a New State of Matter . . . . .</b>	<b>315</b>
30.1	Fibonacci, Noble Numbers and a New State of Matter . . . . .	318
30.2	Cantor Sets, Fractals and a Musical Paradox . . . . .	324
30.3	The Twin Dragon: A Fractal from a Complex Number System . . . . .	329
30.4	Statistical Fractals . . . . .	331
30.5	Some Crazy Mappings . . . . .	333
30.6	The Logistic Parabola and Strange Attractors . . . . .	336
30.7	Conclusion . . . . .	339