

Contents

Part I A Few Fundamentals

1	Introduction	3
	The Family of Numbers	6
1.1	Fibonacci, Continued Fractions and the Golden Ratio	8
1.2	Fermat, Primes and Cyclotomy	11
1.3	Euler, Totients and Cryptography	13
1.4	Gauss, Congruences and Diffraction	14
1.5	Galois, Fields and Codes	16
2	The Natural Numbers	21
2.1	The Fundamental Theorem	21
2.2	The Least Common Multiple	22
2.3	Planetary “Gears”	23
2.4	The Greatest Common Divisor	23
2.5	Human Pitch Perception	25
2.6	Octaves, Temperament, Kilos and Decibels	26
2.7	Coprimes	28
2.8	Euclid’s Algorithm	28
2.9	The Decimal System Decimated	29
3	Primes	31
3.1	How Many Primes are There?	31
3.2	The Sieve of Eratosthenes	32
3.3	A Chinese Theorem in Error	33
3.4	A Formula for Primes	34
3.5	Mersenne Primes	35
3.6	Repunits	39
3.7	Perfect Numbers	39
3.8	Fermat Primes	41
3.9	Gauss and the Impossible Heptagon	42

4	The Prime Distribution	45
4.1	A Probabilistic Argument	45
4.2	The Prime-Counting Function $\pi(x)$	47
4.3	David Hilbert and Large Nuclei	51
4.4	Coprime Probabilities	52
4.5	Primes in Progressions	56
4.6	Primeless Expanses	58
4.7	Squarefree and Coprime Integers	59
4.8	Twin Primes	59
4.9	Prime Triplets	61
4.10	Prime Quadruplets and Quintuplets	62
4.11	Primes at Any Distance	63
4.12	Spacing Distribution Between Adjacent Primes	66
4.13	Goldbach's Conjecture	67
4.14	Sum of Three Primes	68

Part II Some Simple Applications

5	Fractions: Continued, Egyptian and Farey	73
5.1	A Neglected Subject	73
5.2	Relations with Measure Theory	77
5.3	Periodic Continued Fractions	78
5.4	Electrical Networks and Squared Squares	81
5.5	Fibonacci Numbers and the Golden Ratio	83
5.6	Fibonacci, Rabbits and Computers	87
5.7	Fibonacci and Divisibility	90
5.8	Generalized Fibonacci and Lucas Numbers	90
5.9	Egyptian Fractions, Inheritance and Some Unsolved Problems	94
5.10	Farey Fractions	95
	5.10.1 Farey Trees	97
	5.10.2 Locked Pallas	100
5.11	Fibonacci and the Problem of Bank Deposits	102
5.12	Error-Free Computing	103

Part III Congruences and the Like

6	Linear Congruences	111
6.1	Residues	111
6.2	Some Simple Fields	114
6.3	Powers and Congruences	115

- 7 Diophantine Equations** 119
 - 7.1 Relation with Congruences 119
 - 7.2 A Gaussian Trick 120
 - 7.3 A Stamp Problem 122
 - 7.4 Nonlinear Diophantine Equations 124
 - 7.5 Triangular Numbers 125
 - 7.6 Pythagorean Numbers 127
 - 7.7 Exponential Diophantine Equations 128
 - 7.8 Fermat’s Last “Theorem” 129
 - 7.9 The Demise of a Conjecture by Euler 130
 - 7.10 A Nonlinear Diophantine Equation in Physics
and the Geometry of Numbers 131
 - 7.11 Normal-Mode Degeneracy in Room Acoustics
(A Number-Theoretic Application)..... 135
 - 7.12 Waring’s Problem 136

- 8 The Theorems of Fermat, Wilson and Euler** 139
 - 8.1 Fermat’s Theorem 139
 - 8.2 Wilson’s Theorem 140
 - 8.3 Euler’s Theorem 141
 - 8.4 The Impossible Star of David 143
 - 8.5 Dirichlet and Linear Progression 144

- 9 Permutations, Cycles and Derangements** 147
 - 9.1 Permutations 147
 - 9.2 Binomial Coefficients 148
 - 9.3 The Binomial and Related Distributions 149
 - 9.4 Permutation Cycles 150
 - 9.5 Derangements 152
 - 9.6 Ascents and Descents 152
 - 9.7 Quantum Decrypting 153
 - 9.8 Decrypting without Factoring 155
 - 9.9 Quantum Cryptography 156
 - 9.10 One-Time Pads 156
 - 9.11 The Bennet-Brossard Key Distribution Scheme (BB84) 157

Part IV Cryptography and Divisors

- 10 Euler Trap Doors and Public-Key Encryption** 161
 - 10.1 A Numerical Trap Door 163
 - 10.2 Digital Encryption 164
 - 10.3 Public-Key Encryption 165
 - 10.4 A Simple Example 167
 - 10.5 Repeated Encryption 168
 - 10.6 Summary and Encryption Requirements 169

11	The Divisor Functions	171
11.1	The Number of Divisors	171
11.2	The Average of the Divisor Function	174
11.3	The Geometric Mean of the Divisors	174
11.4	The Summatory Function of the Divisor Function	175
11.5	The Generalized Divisor Functions	175
11.6	The Average Value of Euler's Function	176
12	The Prime Divisor Functions	179
12.1	The Number of Different Prime Divisors	179
12.2	The Distribution of $\omega(n)$	182
12.3	The Number of Prime Divisors	185
12.4	The Harmonic Mean of $\Omega(n)$	188
12.5	Medians and Percentiles of $\Omega(n)$	190
12.6	Implications for Public-Key Encryption	191
13	Certified Signatures	193
13.1	A Story of Creative Financing	193
13.2	Certified Signature for Public-Key Encryption	193
14	Primitive Roots	195
14.1	Orders	195
14.2	Periods of Decimal and Binary Fractions	197
14.3	A Primitive Proof of Wilson's Theorem	201
14.4	The Index – A Number-Theoretic Logarithm	201
14.5	Solution of Exponential Congruences	202
14.6	What is the Order T_m of an Integer m Modulo a Prime p ?	204
14.7	Index "Encryption"	205
14.8	A Fourier Property of Primitive Roots and Concert Hall Acoustics	206
14.9	More Spacious-Sounding Sound	207
14.10	Galois Arrays for X-Ray Astronomy	209
14.11	A Negative Property of the Fermat Primes	211
15	Knapsack Encryption	213
15.1	An Easy Knapsack	213
15.2	A Hard Knapsack	214
Part V Residues and Diffraction		
16	Quadratic Residues	219
16.1	Quadratic Congruences	219
16.2	Euler's Criterion	220
16.3	The Legendre Symbol	221
16.4	A Fourier Property of Legendre Sequences	223
16.5	Gauss Sums	224
16.6	Pretty Diffraction	225

16.7	Quadratic Reciprocity	226
16.8	A Fourier Property of Quadratic-Residue Sequences	227
16.9	Spread Spectrum Communication	229
16.10	Generalized Legendre Sequences Obtained Through Complexification of the Euler Criterion	230

Part VI Chinese and Other Fast Algorithms

17	The Chinese Remainder Theorem and Simultaneous Congruences ...	235
17.1	Simultaneous Congruences	235
17.2	The Sino-Representation: A Chinese Number System	236
17.3	Applications of the Sino-Representation	237
17.4	Discrete Fourier Transformation in Sino	239
17.5	A Sino-Optical Fourier Transformer	240
17.6	Generalized Sino-Representation	241
17.7	Fast Prime-Length Fourier Transform	242
18	Fast Transformation and Kronecker Products	245
18.1	A Fast Hadamard Transform	245
18.2	The Basic Principle of the Fast Fourier Transforms	248
19	Quadratic Congruences	251
19.1	Application of the Chinese Remainder Theorem (CRT)	251

Part VII Pseudoprimes, Möbius Transform, and Partitions

20	Pseudoprimes, Poker and Remote Coin Tossing	255
20.1	Pulling Roots to Ferret Out Composites	255
20.2	Factors from a Square Root	257
20.3	Coin Tossing by Telephone	258
20.4	Absolute and Strong Pseudoprimes	260
20.5	Fermat and Strong Pseudoprimes	262
20.6	Deterministic Primality Testing	263
20.7	A Very Simple Factoring Algorithm	264
20.8	Factoring with Elliptic Curves	265
20.9	Quantum Factoring	265
21	The Möbius Function and the Möbius Transform	267
21.1	The Möbius Transform and Its Inverse	268
21.2	Proof of the Inversion Formula	269
21.3	Second Inversion Formula	270
21.4	Third Inversion Formula	271
21.5	Fourth Inversion Formula	271
21.6	Riemann's Hypothesis and the Disproof of the Mertens Conjecture	271
21.7	Dirichlet Series and the Möbius Function	272

22	Generating Functions and Partitions	275
22.1	Generating Functions	275
22.2	Partitions of Integers	277
22.3	Generating Functions of Partitions	278
22.4	Restricted Partitions	279
23	From Error Correcting Codes to Covering Sets	283
23.1	Covering Sets in Coding Theory	283
23.2	Discrete Covering Sets	284
Part VIII Cyclotomy and Polynomials		
24	Cyclotomic Polynomials	289
24.1	How to Divide a Circle into Equal Parts	289
24.2	Gauss's Great Insight	292
24.3	Factoring in Different Fields	296
24.4	Cyclotomy in the Complex Plane	297
24.5	How to Divide a Circle with Compass and Straightedge	298
24.5.1	Rational Factors of $z^N - 1$	299
24.6	An Alternative Rational Factorization	301
24.7	Relation Between Rational Factors and Complex Roots	301
24.8	How to Calculate with Cyclotomic Polynomials	303
25	Linear Systems and Polynomials	305
25.1	Impulse Responses	305
25.2	Time-Discrete Systems and the z Transform	306
25.3	Discrete Convolution	306
25.4	Cyclotomic Polynomials and z Transform	307
26	Polynomial Theory	309
26.1	Some Basic Facts of Polynomial Life	309
26.2	Polynomial Residues	310
26.3	Chinese Remainders for Polynomials	312
26.4	Euclid's Algorithm for Polynomials	313
Part IX Galois Fields and More Applications		
27	Galois Fields	317
27.1	Prime Order	317
27.2	Prime Power Order	317
27.3	Generation of $GF(2^4)$	320
27.4	How Many Primitive Elements?	321
27.5	Recursive Relations	321
27.6	How to Calculate in $GF(p^m)$	324
27.7	Zech Logarithm, Doppler Radar and Optimum Ambiguity Functions	324

27.8	A Unique Phase-Array Based on the Zech Logarithm	327
27.9	Spread-Spectrum Communication and Zech Logarithms	328
28	Spectral Properties of Galois Sequences	331
28.1	Circular Correlation	331
28.2	Application to Error-Correcting Codes and Speech Recognition . .	333
28.3	Application to Precision Measurements	335
28.4	Concert Hall Measurements	336
28.5	The Fourth Effect of General Relativity	336
28.6	Toward Better Concert Hall Acoustics	338
28.7	Higher-Dimensional Diffusors	343
28.8	Active Array Applications	344
29	Random Number Generators	347
29.1	Pseudorandom Galois Sequences	348
29.2	Randomness from Congruences	349
29.3	“Continuous” Distributions	350
29.4	Four Ways to Generate a Gaussian Variable	351
29.5	Pseudorandom Sequences in Cryptography	352
30	Waveforms and Radiation Patterns	355
30.1	Special Phases	356
30.2	The Rudin-Shapiro Polynomials	358
30.3	Gauss Sums and Peak Factors	359
30.4	Galois Sequences and the Smallest Peak Factors	361
30.5	Minimum Redundancy Antennas	363
30.6	Golomb Rulers	365
31	Number Theory, Randomness and “Art”	367
31.1	Number Theory and Graphic Design	367
31.2	The Primes of Gauss and Eisenstein	369
31.3	Galois Fields and Impossible Necklaces	370
31.4	“Baroque” Integers	374
Part X Self-Similarity, Fractals and Art		
32	Self-Similarity, Fractals, Deterministic Chaos and a New State of Matter	379
32.1	Fibonacci, Noble Numbers and a New State of Matter	382
32.2	Cantor Sets, Fractals and a Musical Paradox	388
32.3	The Twin Dragon: A Fractal from a Complex Number System. . .	394
32.4	Statistical Fractals	395
32.5	Some Crazy Mappings	397
32.6	The Logistic Parabola and Strange Attractors	399
32.7	Conclusion	403

Glossary of Symbols 405

References 409

Name Index 419

Subject Index 423