

Contents

Part I. A Few Fundamentals

1. Introduction	1
1.1 Fibonacci, Continued Fractions and the Golden Ratio	4
1.2 Fermat, Primes and Cyclotomy	6
1.3 Euler, Totients and Cryptography	8
1.4 Gauss, Congruences and Diffraction	10
1.5 Galois, Fields and Codes	11
2. The Natural Numbers	16
2.1 The Fundamental Theorem	16
2.2 The Least Common Multiple	17
2.3 Planetary “Gears”	18
2.4 The Greatest Common Divisor	18
2.5 Human Pitch Perception	20
2.6 Octaves, Temperament, Kilos and Decibels	21
2.7 Coprimes	23
2.8 Euclid’s Algorithm	23
3. Primes	25
3.1 How Many Primes are There?	25
3.2 The Sieve of Eratosthenes	26
3.3 A Chinese Theorem in Error	27
3.4 A Formula for Primes	28
3.5 Mersenne Primes	29
3.6 Repunits	33
3.7 Perfect Numbers	34
3.8 Fermat Primes	35
3.9 Gauss and the Impossible Heptagon	36
4. The Prime Distribution	38
4.1 A Probabilistic Argument	38
4.2 The Prime-Counting Function $\pi(x)$	40
4.3 David Hilbert and Large Nuclei	44
4.4 Coprime Probabilities	45

4.5	Primes in Progressions	48
4.6	Primeless Expanses	50
4.7	Squarefree and Coprime Integers	51
4.8	Twin Primes	51
4.9	Prime Triplets	53
4.10	Prime Quadruplets and Quintuplets	54
4.11	Primes at Any Distance	55
4.12	Spacing Distribution Between Adjacent Primes	58
4.13	Goldbach's Conjecture	58
4.14	Sum of Three Primes	60

Part II. Some Simple Applications

5.	Fractions: Continued, Egyptian and Farey	62
5.1	A Neglected Subject	62
5.2	Relations with Measure Theory	66
5.3	Periodic Continued Fractions	67
5.4	Electrical Networks and Squared Squares	70
5.5	Fibonacci Numbers and the Golden Ratio	71
5.6	Fibonacci, Rabbits and Computers	75
5.7	Fibonacci and Divisibility	77
5.8	Generalized Fibonacci and Lucas Numbers	78
5.9	Egyptian Fractions, Inheritance and Some Unsolved Problems	81
5.10	Farey Fractions	82
5.10.1	Farey Trees	85
5.10.2	Locked Pallas	88
5.11	Fibonacci and the Problem of Bank Deposits	89
5.12	Error-Free Computing	90

Part III. Congruences and the Like

6.	Linear Congruences	95
6.1	Residues	95
6.2	Some Simple Fields	98
6.3	Powers and Congruences	99
7.	Diophantine Equations	102
7.1	Relation with Congruences	102
7.2	A Gaussian Trick	103
7.3	Nonlinear Diophantine Equations	105
7.4	Triangular Numbers	106
7.5	Pythagorean Numbers	108

7.6	Exponential Diophantine Equations	109
7.7	Fermat's Last "Theorem"	109
7.8	The Demise of a Conjecture by Euler	111
7.9	A Nonlinear Diophantine Equation in Physics and the Geometry of Numbers	111
7.10	Normal-Mode Degeneracy in Room Acoustics (A Number-Theoretic Application)	115
7.11	Waring's Problem	116
8.	The Theorems of Fermat, Wilson and Euler	118
8.1	Fermat's Theorem	118
8.2	Wilson's Theorem	119
8.3	Euler's Theorem	120
8.4	The Impossible Star of David	121
8.5	Dirichlet and Linear Progression	123
Part IV. Cryptography and Divisors		
9.	Euler Trap Doors and Public-Key Encryption	125
9.1	A Numerical Trap Door	127
9.2	Digital Encryption	128
9.3	Public-Key Encryption	129
9.4	A Simple Example	131
9.5	Repeated Encryption	132
9.6	Summary and Encryption Requirements	133
10.	The Divisor Functions	135
10.1	The Number of Divisors	135
10.2	The Average of the Divisor Function	138
10.3	The Geometric Mean of the Divisors	138
10.4	The Summatory Function of the Divisor Function	139
10.5	The Generalized Divisor Functions	139
10.6	The Average Value of Euler's Function	140
11.	The Prime Divisor Functions	142
11.1	The Number of Different Prime Divisors	142
11.2	The Distribution of $\omega(n)$	146
11.3	The Number of Prime Divisors	147
11.4	The Harmonic Mean of $\Omega(n)$	150
11.5	Medians and Percentiles of $\Omega(n)$	152
11.6	Implications for Public-Key Encryption	153

12. Certified Signatures	154
12.1 A Story of Creative Financing	154
12.2 Certified Signature for Public-Key Encryption	154
13. Primitive Roots	156
13.1 Orders	156
13.2 Periods of Decimal and Binary Fractions	159
13.3 A Primitive Proof of Wilson's Theorem	162
13.4 The Index – A Number-Theoretic Logarithm	162
13.5 Solution of Exponential Congruences	163
13.6 What is the Order T_m of an Integer m Modulo a Prime p ?	165
13.7 Index "Encryption"	166
13.8 A Fourier Property of Primitive Roots and Concert Hall Acoustics	166
13.9 More Spacious-Sounding Sound	168
13.10 Galois Arrays for X-Ray Astronomy	170
13.11 A Negative Property of the Fermat Primes	171
14. Knapsack Encryption	173
14.1 An Easy Knapsack	173
14.2 A Hard Knapsack	174

Part V. Residues and Diffraction

15. Quadratic Residues	177
15.1 Quadratic Congruences	177
15.2 Euler's Criterion	178
15.3 The Legendre Symbol	179
15.4 A Fourier Property of Legendre Sequences	181
15.5 Gauss Sums	181
15.6 Pretty Diffraction	183
15.7 Quadratic Reciprocity	183
15.8 A Fourier Property of Quadratic-Residue Sequences	184
15.9 Spread Spectrum Communication	186
15.10 Generalized Legendre Sequences Obtained Through Complexification of the Euler Criterion	187

Part VI. Chinese and Other Fast Algorithms

16. The Chinese Remainder Theorem and Simultaneous Congruences	190
16.1 Simultaneous Congruences	190
16.2 The Sino-Representation: A Chinese Number System	191

16.3	Applications of the Sino-Representation	192
16.4	Discrete Fourier Transformation in Sino	194
16.5	A Sino-Optical Fourier Transformer	195
16.6	Generalized Sino-Representation	196
16.7	Fast Prime-Length Fourier Transform	197
17.	Fast Transformation and Kronecker Products	199
17.1	A Fast Hadamard Transform	199
17.2	The Basic Principle of the Fast Fourier Transforms	202
18.	Quadratic Congruences	203
18.1	Application of the Chinese Remainder Theorem (CRT)	203
Part VII. Pseudoprimes, Möbius Transform, and Partitions		
19.	Pseudoprimes, Poker and Remote Coin Tossing	205
19.1	Pulling Roots to Ferret Out Composites	205
19.2	Factors from a Square Root	206
19.3	Coin Tossing by Telephone	208
19.4	Absolute and Strong Pseudoprimes	210
19.5	Fermat and Strong Pseudoprimes	212
19.6	Deterministic Primality Testing	212
19.7	A Very Simple Factoring Algorithm	214
19.8	Factoring with Elliptic Curves	214
19.9	Quantum Factoring	215
20.	The Möbius Function and the Möbius Transform	216
20.1	The Möbius Transform and Its Inverse	216
20.2	Proof of the Inversion Formula	218
20.3	Second Inversion Formula	219
20.4	Third Inversion Formula	219
20.5	Fourth Inversion Formula	220
20.6	Riemann's Hypothesis and the Disproof of the Mertens Conjecture	220
20.7	Dirichlet Series and the Möbius Function	221
21.	Generating Functions and Partitions	224
21.1	Generating Functions	224
21.2	Partitions of Integers	226
21.3	Generating Functions of Partitions	227
21.4	Restricted Partitions	228

Part VIII. Cyclotomy and Polynomials

22. Cyclotomic Polynomials	232
22.1 How to Divide a Circle into Equal Parts	232
22.2 Gauss's Great Insight	235
22.3 Factoring in Different Fields	239
22.4 Cyclotomy in the Complex Plane	239
22.5 How to Divide a Circle with Compass and Straightedge	240
22.5.1 Rational Factors of $z^N - 1$	242
22.6 An Alternative Rational Factorization	243
22.7 Relation Between Rational Factors and Complex Roots	244
22.8 How to Calculate with Cyclotomic Polynomials	245
23. Linear Systems and Polynomials	247
23.1 Impulse Responses	247
23.2 Time-Discrete Systems and the z Transform	248
23.3 Discrete Convolution	248
23.4 Cyclotomic Polynomials and z Transform	249
24. Polynomial Theory	250
24.1 Some Basic Facts of Polynomial Life	250
24.2 Polynomial Residues	251
24.3 Chinese Remainders for Polynomials	252
24.4 Euclid's Algorithm for Polynomials	253

Part IX. Galois Fields and More Applications

25. Galois Fields	256
25.1 Prime Order	256
25.2 Prime Power Order	256
25.3 Generation of $GF(2^4)$	258
25.4 How Many Primitive Elements?	260
25.5 Recursive Relations	260
25.6 How to Calculate in $GF(p^m)$	262
25.7 Zech Logarithm, Doppler Radar and Optimum Ambiguity Functions	263
25.8 A Unique Phase-Array Based on the Zech Logarithm	266
25.9 Spread-Spectrum Communication and Zech Logarithms	268
26. Spectral Properties of Galois Sequences	269
26.1 Circular Correlation	269
26.2 Application to Error-Correcting Codes and Speech Recognition	271

26.3	Application to Precision Measurements	273
26.4	Concert Hall Measurements	274
26.5	The Fourth Effect of General Relativity	275
26.6	Toward Better Concert Hall Acoustics	276
26.7	Higher-Dimensional Diffusors	281
26.8	Active Array Applications	282
27.	Random Number Generators	283
27.1	Pseudorandom Galois Sequences	284
27.2	Randomness from Congruences	285
27.3	"Continuous" Distributions	286
27.4	Four Ways to Generate a Gaussian Variable	287
27.5	Pseudorandom Sequences in Cryptography	288
28.	Waveforms and Radiation Patterns	289
28.1	Special Phases	290
28.2	The Rudin-Shapiro Polynomials	292
28.3	Gauss Sums and Peak Factors	293
28.4	Galois Sequences and the Smallest Peak Factors	295
28.5	Minimum Redundancy Antennas	297
28.6	Golomb Rulers	299
29.	Number Theory, Randomness and "Art"	301
29.1	Number Theory and Graphic Design	301
29.2	The Primes of Gauss and Eisenstein	303
29.3	Galois Fields and Impossible Necklaces	304
29.4	"Baroque" Integers	308

Part X. Self-Similarity, Fractals and Art

30.	Self-Similarity, Fractals, Deterministic Chaos and a New State of Matter	311
30.1	Fibonacci, Noble Numbers and a New State of Matter	315
30.2	Cantor Sets, Fractals and a Musical Paradox	320
30.3	The Twin Dragon: A Fractal from a Complex Number System	325
30.4	Statistical Fractals	327
30.5	Some Crazy Mappings	329
30.6	The Logistic Parabola and Strange Attractors	332
30.7	Conclusion	335

Glossary of Symbols	336
References	339
Name Index	351
Subject Index	355