

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	7
1.3 Euler, Totients and Cryptography	9
1.4 Gauss, Congruences and Diffraction	10
1.5 Galois, Fields and Codes	12
2. The Natural Numbers	17
2.1 The Fundamental Theorem	17
2.2 The Least Common Multiple	18
2.3 Planetary “Gears”	19
2.4 The Greatest Common Divisor	20
2.5 Human Pitch Perception	22
2.6 Octaves, Temperament, Kilos and Decibels	22
2.7 Coprimes	25
2.8 Euclid’s Algorithm	25
3. Primes	26
3.1 How Many Primes are There?	26
3.2 The Sieve of Eratosthenes	27
3.3 A Chinese Theorem in Error	29
3.4 A Formula for Primes	29
3.5 Mersenne Primes	30
3.6 Repunits	34
3.7 Perfect Numbers	35
3.8 Fermat Primes	37
3.9 Gauss and the Impossible Heptagon	38
4. The Prime Distribution	40
4.1 A Probabilistic Argument	40
4.2 The Prime-Counting Function $\pi(x)$	43
4.3 David Hilbert and Large Nuclei	47
4.4 Coprime Probabilities	48

4.5	Twin Primes	51
4.6	Primeless Expanses	53
4.7	Square-Free and Coprime Integers	54

Part II Some Simple Applications

5. Fractions: Continued, Egyptian and Farey	55
5.1 A Neglected Subject	55
5.2 Relations with Measure Theory	60
5.3 Periodic Continued Fractions	60
5.4 Electrical Networks and Squared Squares	64
5.5 Fibonacci Numbers and the Golden Ratio	65
5.6 Fibonacci, Rabbits and Computers	70
5.7 Fibonacci and Divisibility	72
5.8 Generalized Fibonacci and Lucas Numbers	73
5.9 Egyptian Fractions, Inheritance and Some Unsolved Problems	76
5.10 Farey Fractions	77
5.11 Fibonacci and the Problem of Bank Deposits	80
5.12 Error-Free Computing	81

Part III Congruences and the Like

6. Linear Congruences	87
6.1 Residues	87
6.2 Some Simple Fields	90
6.3 Powers and Congruences	92
7. Diophantine Equations	95
7.1 Relation with Congruences	95
7.2 A Gaussian Trick	96
7.3 Nonlinear Diophantine Equations	98
7.4 Triangular Numbers	100
7.5 Pythagorean Numbers	102
7.6 Exponential Diophantine Equations	103
7.7 Fermat's Last "Theorem"	104
7.8 The Demise of a Conjecture by Euler	105
7.9 A Nonlinear Diophantine Equation in Physics and the Geometry of Numbers	106
7.10 Normal-Mode Degeneracy in Room Acoustics (A Number-Theoretic Application)	108
7.11 Waring's Problem	109

8. The Theorems of Fermat, Wilson and Euler	111
8.1 Fermat's Theorem	111
8.2 Wilson's Theorem	112
8.3 Euler's Theorem	113
8.4 The Impossible Star of David	115
8.5 Dirichlet and Linear Progression	116

Part IV Cryptography and Divisors

9. Euler Trap Doors and Public-Key Encryption	118
9.1 A Numerical Trap Door	118
9.2 Digital Encryption	119
9.3 Public-Key Encryption	121
9.4 A Simple Example	123
9.5 Repeated Encryption	123
9.6 Summary and Encryption Requirements	125
10. The Divisor Functions	127
10.1 The Number of Divisors	127
10.2 The Average of the Divisor Function	130
10.3 The Geometric Mean of the Divisors	131
10.4 The Summatory Function of the Divisor Function	131
10.5 The Generalized Divisor Functions	132
10.6 The Average Value of Euler's Function	133
11. The Prime Divisor Functions	135
11.1 The Number of Different Prime Divisors	135
11.2 The Distribution of $\omega(n)$	138
11.3 The Number of Prime Divisors	141
11.4 The Harmonic Mean of $\Omega(n)$	144
11.5 Medians and Percentiles of $\Omega(n)$	146
11.6 Implications for Public-Key Encryption	147
12. Certified Signatures	149
12.1 A Story of Creative Financing	149
12.2 Certified Signature for Public-Key Encryption	149
13. Primitive Roots	151
13.1 Orders	151
13.2 Periods of Decimal and Binary Fractions	154
13.3 A Primitive Proof of Wilson's Theorem	157
13.4 The Index – A Number-Theoretic Logarithm	158
13.5 Solution of Exponential Congruences	159
13.6 What is the Order T_m of an Integer m Modulo a Prime p ? ..	161
13.7 Index "Encryption"	162

13.8	A Fourier Property of Primitive Roots and Concert Hall Acoustics	163
13.9	More Spacious-Sounding Sound	164
13.10	A Negative Property of the Fermat Primes	167
14.	Knapsack Encryption	168
14.1	An Easy Knapsack	168
14.2	A Hard Knapsack	169

Part V Residues and Diffraction

15.	Quadratic Residues	172
15.1	Quadratic Congruences	172
15.2	Euler's Criterion	173
15.3	The Legendre Symbol	175
15.4	A Fourier Property of Legendre Sequences	176
15.5	Gauss Sums	177
15.6	Pretty Diffraction	179
15.7	Quadratic Reciprocity	179
15.8	A Fourier Property of Quadratic-Residue Sequences	180
15.9	Spread Spectrum Communication	183
15.10	Generalized Legendre Sequences Obtained Through Complexification of the Euler Criterion	183

Part VI Chinese and Other Fast Algorithms

16.	The Chinese Remainder Theorem and Simultaneous Congruences ..	186
16.1	Simultaneous Congruences	186
16.2	The Sino-Representation: A Chinese Number System	187
16.3	Applications of the Sino-Representation	189
16.4	Discrete Fourier Transformation in Sino	190
16.5	A Sino-Optical Fourier Transformer	191
16.6	Generalized Sino-Representation	192
16.7	Fast Prime-Length Fourier Transform	194
17.	Fast Transformations and Kronecker Products	196
17.1	A Fast Hadamard Transform	196
17.2	The Basic Principle of the Fast Fourier Transforms	199
18.	Quadratic Congruences	201
18.1	Application of the Chinese Remainder Theorem (CRT)	201

Part VII Pseudoprimes, Möbius Transform, and Partitions

19. Pseudoprimes, Poker and Remote Coin Tossing	203
19.1 Pulling Roots to Ferret Out Composites	203
19.2 Factors from a Square Root	205
19.3 Coin Tossing by Telephone	206
19.4 Absolute and Strong Pseudoprimes	209
19.5 Fermat and Strong Pseudoprimes	211
19.6 Deterministic Primality Testing	212
19.7 A Very Simple Factoring Algorithm	213
20. The Möbius Function and the Möbius Transform	215
20.1 The Möbius Transform and Its Inverse	215
20.2 Proof of the Inversion Formula	217
20.3 Second Inversion Formula	218
20.4 Third Inversion Formula	219
20.5 Fourth Inversion Formula	219
20.6 Riemann's Hypothesis and the Disproof of the Mertens Conjecture	219
20.7 Dirichlet Series and the Möbius Function	220
21. Generating Functions and Partitions	223
21.1 Generating Functions	223
21.2 Partitions of Integers	225
21.3 Generating Functions of Partitions	226
21.4 Restricted Partitions	227

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	240
22.4 Cyclotomy in the Complex Plane	240
22.5 How to Divide a Circle with Compass and Straightedge	242
22.5.1 Rational Factors of $z^N - 1$	243
22.6 An Alternative Rational Factorization	244
22.7 Relation Between Rational Factors and Complex Roots	245
22.8 How to Calculate with Cyclotomic Polynomials	247
23. Linear Systems and Polynomials	249
23.1 Impulse Responses	249
23.2 Time-Discrete Systems and the z Transform	250

23.3	Discrete Convolution	251
23.4	Cyclotomic Polynomials and z Transform	251
24.	Polynomial Theory	253
24.1	Some Basic Facts of Polynomial Life	253
24.2	Polynomial Residues	254
24.3	Chinese Remainders for Polynomials	256
24.4	Euclid's Algorithm for Polynomials	257

Part IX Galois Fields and More Applications

25.	Galois Fields	259
25.1	Prime Order	259
25.2	Prime Power Order	259
25.3	Generation of $GF(2^4)$	262
25.4	How Many Primitive Elements?	263
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	271
25.9	Spread-Spectrum Communication and Zech Logarithms ...	272
26.	Spectral Properties of Galois Sequences	274
26.1	Circular Correlation	274
26.2	Application to Error-Correcting Codes and Speech Recognition	277
26.3	Application to Precision Measurements	278
26.4	Concert Hall Measurements	279
26.5	The Fourth Effect of General Relativity	280
26.6	Toward Better Concert Hall Acoustics	281
26.7	Higher-Dimensional Diffusors	287
26.8	Active Array Applications	287
27.	Random Number Generators	289
27.1	Pseudorandom Galois Sequences	290
27.2	Randomness from Congruences	291
27.3	"Continuous" Distributions	292
27.4	Four Ways to Generate a Gaussian Variable	293
27.5	Pseudorandom Sequences in Cryptography	295
28.	Waveforms and Radiation Patterns	296
28.1	Special Phases	297
28.2	The Rudin-Shapiro Polynomials	299
28.3	Gauss Sums and Peak Factors	300

28.4	Galois Sequences and the Smallest Peak Factors	302
28.5	Minimum Redundancy Antennas	305
29.	Number Theory, Randomness and "Art"	307
29.1	Number Theory and Graphic Design	307
29.2	The Primes of Gauss and Eisenstein	309
29.3	Galois Fields and Impossible Necklaces	310

Part X Self Similarity, Fractals and Art

30.	Self-Similarity, Fractals, Deterministic Chaos and a New State of Matter	315
30.1	Fibonacci, Noble Numbers and a New State of Matter	319
30.2	Cantor Sets, Fractals and a Musical Paradox	324
30.3	The Twin Dragon: a Fractal from a Complex Number System	330
30.4	Statistical Fractals	331
30.5	Some Crazy Mappings	333
30.6	The Logistic Parabola and Strange Attractors	337
30.7	Conclusion	340
Appendix		341
A.	A Calculator Program for Exponentiation and Residue Reduction	341
B.	A Calculator Program for Calculating Fibonacci and Lucas Numbers	345
C.	A Calculator Program for Decomposing an Integer According to the Fibonacci Number System	346
Glossary of Symbols		349
References		353
Name Index		363
Subject Index		367