

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	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	24
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	30
3.5 Mersenne Primes	31
3.6 Repunits	35
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

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	63
5.5 Fibonacci Numbers and the Golden Ratio	64
5.6 Fibonacci, Rabbits and Computers	69
5.7 Fibonacci and Divisibility	71
5.8 Generalized Fibonacci and Lucas Numbers	72
5.9 Egyptian Fractions, Inheritance and Some Unsolved Problems	75
5.10 Farey Fractions	76

Part III Congruences and the Like

6. Linear Congruences	79
6.1 Residues	79
6.2 Some Simple Fields	82
6.3 Powers and Congruences	84
7. Diophantine Equations	87
7.1 Relation with Congruences	87
7.2 A Gaussian Trick	88
7.3 Nonlinear Diophantine Equations	90
7.4 Triangular Numbers	91
7.5 Pythagorean Numbers	93
7.6 Exponential Diophantine Equations	94
7.7 Fermat's Last "Theorem"	95
7.8 The Demise of a Conjecture by Euler	97
7.9 A Nonlinear Diophantine Equation in Physics and the Geometry of Numbers	97
7.10 Normal-Mode Degeneracy in Room Acoustics (A Number-Theoretic Application)	100
7.11 Waring's Problem	100
8. The Theorems of Fermat, Wilson and Euler	102
8.1 Fermat's Theorem	102
8.2 Wilson's Theorem	103
8.3 Euler's Theorem	104
8.4 The Impossible Star of David	106
8.5 Dirichlet and Linear Progression	108

Part IV Cryptography and Divisors

9. Euler Trap Doors and Public-Key Encryption	110
9.1 A Numerical Trap Door	110
9.2 Digital Encryption	111
9.3 Public-Key Encryption	113
9.4 A Simple Example	115
9.5 Repeated Encryption	115
9.6 Summary and Encryption Requirements	117
10. The Divisor Functions	119
10.1 The Number of Divisors	119
10.2 The Average of the Divisor Function	122
10.3 The Geometric Mean of the Divisor Function	123
10.4 The Summatory Function of the Divisor Function	123
10.5 The Generalized Divisor Functions	124
10.6 The Average Value of Euler's Function	124
11. The Prime Divisor Functions	127
11.1 The Number of Different Prime Divisors	127
11.2 The Distribution of $\omega(n)$	130
11.3 The Number of Prime Divisors	133
11.4 The Harmonic Mean of $\Omega(n)$	136
11.5 Medians and Percentiles of $\Omega(n)$	138
11.6 Implications for Public-Key Encryption	139
12. Certified Signatures	141
12.1 A Story of Creative Financing	141
12.2 Certified Signature for Public-Key Encryption	141
13. Primitive Roots	143
13.1 Orders	143
13.2 Periods of Decimals and Binary Fractions	146
13.3 A Primitive Proof of Wilson's Theorem	149
13.4 The Index – A Number-Theoretic Logarithm	150
13.5 Solution of Exponential Congruences	151
13.6 What is the Order T_m of an Integer m Modulo a Prime p ?	153
13.7 Index "Encryption"	154
13.8 A Fourier Property of Primitive Roots and Concert Hall Acoustics	155
13.9 More Spacious-Sounding Sound	156
14. Knapsack Encryption	160
14.1 An Easy Knapsack	160
14.2 A Hard Knapsack	161

Part V Residues and Diffraction

15. Quadratic Residues	164
15.1 Quadratic Congruences	164
15.2 Euler's Criterion	165
15.3 The Legendre Symbol	167
15.4 A Fourier Property of Legendre Sequences	168
15.5 Gauss Sums	169
15.6 Pretty Diffraction	171
15.7 Quadratic Reciprocity	171
15.8 A Fourier Property of Quadratic-Residue Sequences	172
15.9 Spread Spectrum Communication	175

Part VI Chinese and Other Fast Algorithms

16. The Chinese Remainder Theorem and Simultaneous Congruences ..	176
16.1 Simultaneous Congruences	176
16.2 The Sino-Representation: A Chinese Number System	177
16.3 Applications of the Sino-Representation	179
16.4 Discrete Fourier Transformation in Sino	180
16.5 A Sino-Optical Fourier Transformer	181
16.6 Generalized Sino-Representation	182
16.7 Fast Prime-Length Fourier Transform	184
17. Fast Transformations and Kronecker Products	186
17.1 A Fast Hadamard Transform	186
17.2 The Basic Principle of the Fast Fourier Transforms	189
18. Quadratic Congruences	191
18.1 Application of the Chinese Remainder Theorem (CRT)	191

Part VII Pseudoprimes, Möbius Transform, and Partitions

19. Pseudoprimes, Poker and Remote Coin Tossing	193
19.1 Pulling Roots to Ferret Out Composites	193
19.2 Factors from a Square Root	195
19.3 Coin Tossing by Telephone	196
19.4 Absolute and Strong Pseudoprimes	199
19.5 Fermat and Strong Pseudoprimes	201
19.6 Deterministic Primality Testing	202
20. The Möbius Function and the Möbius Transform	204
20.1 The Möbius Transform and Its Inverse	204
20.2 Proof of the Inversion Formula	206

20.3	Second Inversion Formula	207
20.4	Third Inversion Formula	208
20.5	Fourth Inversion Formula	208
20.6	Special Infinite Sums	208
20.7	Dirichlet Series and the Möbius Functions	209
21.	Generating Functions and Partitions	212
21.1	Generating Functions	212
21.2	Partitions of Integers	214
21.3	Generating Functions of Partitions	215
21.4	Restricted Partitions	216

Part VIII Cyclotomy and Polynomials

22.	Cyclotomic Polynomials	221
22.1	How to Divide a Circle into Equal Parts	221
22.2	Gauss's Great Insight	224
22.3	Factoring in Different Fields	229
22.4	Cyclotomy in the Complex Plane	229
22.5	How to Divide a Circle with Compass and Straightedge	231
	22.5.1 Rational Factors of $z^N - 1$	232
22.6	An Alternative Rational Factorization	233
22.7	Relation Between Rational Factors and Complex Roots	234
22.8	How to Calculate with Cyclotomic Polynomials	236
23.	Linear Systems and Polynomials	238
23.1	Impulse Responses	238
23.2	Time-Discrete Systems and the z Transform	239
23.3	Discrete Convolution	240
23.4	Cyclotomic Polynomials and z Transform	240
24.	Polynomial Theory	242
24.1	Some Basic Facts of Polynomial Life	242
24.2	Polynomial Residues	243
24.3	Chinese Remainders for Polynomials	245
24.4	Euclid's Algorithm for Polynomials	246

Part IX Galois Fields and More Applications

25.	Galois Fields	248
25.1	Prime Order	248
25.2	Prime Power Order	248
25.3	Generation of $GF(2^4)$	251
25.4	How Many Primitive Elements?	252

25.5	Recursive Relations	253
25.6	How to Calculate in $GF(p^m)$	254
26.	Spectral Properties of Galois Sequences	256
26.1	Circular Correlation	256
26.2	Application to Error-Correcting Codes	259
26.3	Application to Precision Measurements	260
26.4	Concert Hall Measurements	261
26.5	The Fourth Effect of General Relativity	262
26.6	Toward Better Concert Hall Acoustics	263
26.7	Higher-Dimensional Diffusers	268
26.8	Active Array Applications	269
27.	Random Number Generators	271
27.1	Pseudorandom Galois Sequences	272
27.2	Randomness from Congruences	273
27.3	“Continuous” Distributions	274
27.4	Four Ways to Generate a Gaussian Variable	275
27.5	Pseudorandom Sequences in Cryptography	277
28.	Waveforms and Radiation Patterns	278
28.1	Special Phases	279
28.2	The Rudin-Shapiro Polynomials	281
28.3	Gauss Sums and Peak Factors	282
28.4	Galois Sequences and the Smallest Peak Factors	284
28.5	Minimum Redundancy Antennas	287
29.	Number Theory, Randomness and “Art”	289
29.1	Number Theory and Graphic Design	289
29.2	The Primes of Gauss and Eisenstein	291
29.3	Galois Theory and Impossible Necklaces	292
30.	Conclusion	297
Appendix		298
A.	A Calculator Program for Exponentiation and Residue Reduction	298
B.	A Calculator Program for Calculating Fibonacci and Lucas Numbers	302
C.	A Calculator Program for Decomposing an Integer According to the Fibonacci Number System	303
Glossary of Symbols		306
References		309
Subject Index		319