

Introduction	1
1 A Brief History of Prime	7
1.1 Euclid and Primes	7
1.2 Summing Over the Primes	11
1.3 Listing the Primes	16
1.4 Fermat Numbers	29
1.5 Primality Testing	31
1.6 Proving the Fundamental Theorem of Arithmetic	35
1.7 Euclid's Theorem Revisited	39
2 Diophantine Equations	43
2.1 Pythagoras	43
2.2 The Fundamental Theorem of Arithmetic in Other Contexts	45
2.3 Sums of Squares	48
2.4 Siegel's Theorem	52
2.5 Fermat, Catalan, and Euler	56
3 Quadratic Diophantine Equations	59
3.1 Quadratic Congruences	59
3.2 Euler's Criterion	65
3.3 The Quadratic Reciprocity Law	67
3.4 Quadratic Rings	73
3.5 Units in $\mathbb{Z}[\sqrt{d}]$, $d > 0$	75
3.6 Quadratic Forms	78
4 Recovering the Fundamental Theorem of Arithmetic	83
4.1 Crisis	83
4.2 An Ideal Solution	84
4.3 Fundamental Theorem of Arithmetic for Ideals	85

4.4	The Ideal Class Group	89
5	Elliptic Curves	93
5.1	Rational Points	93
5.2	The Congruent Number Problem	98
5.3	Explicit Formulas	105
5.4	Points of Order Eleven	110
5.5	Prime Values of Elliptic Divisibility Sequences	112
5.6	Ramanujan Numbers and the Taxicab Problem	117
6	Elliptic Functions	121
6.1	Elliptic Functions	121
6.2	Parametrizing an Elliptic Curve	126
6.3	Complex Torsion	128
6.4	Partial Proof of Theorem 6.5	129
7	Heights	133
7.1	Heights on Elliptic Curves	133
7.2	Mordell's Theorem	138
7.3	The Weak Mordell Theorem: Congruent Number Curve	142
7.4	The Parallelogram Law and the Canonical Height	146
7.5	Mahler Measure and the Naïve Parallelogram Law	150
8	The Riemann Zeta Function	157
8.1	Euler's Summation Formula	158
8.2	Multiplicative Arithmetic Functions	161
8.3	Dirichlet Convolution	164
8.4	Euler Products	169
8.5	Uniform Convergence	171
8.6	The Zeta Function Is Analytic	173
8.7	Analytic Continuation of the Zeta Function	175
9	The Functional Equation of the Riemann Zeta Function	183
9.1	The Gamma Function	183
9.2	The Functional Equation	185
9.3	Fourier Analysis on Schwartz Spaces	187
9.4	Fourier Analysis of Periodic Functions	189
9.5	The Theta Function	194
9.6	The Gamma Function Revisited	197

10 Primes in an Arithmetic Progression	207
10.1 A New Method of Proof	208
10.2 Congruences Modulo 3	211
10.3 Characters of Finite Abelian Groups	213
10.4 Dirichlet Characters and L -Functions	217
10.5 Analytic Continuation and Abel's Summation Formula	219
10.6 Abel's Limit Theorem	223
11 Converging Streams	225
11.1 The Class Number Formula	225
11.2 The Dedekind Zeta Function	229
11.3 Proof of the Class Number Formula	233
11.4 The Sign of the Gauss Sum	235
11.5 The Conjectures of Birch and Swinnerton-Dyer	238
12 Computational Number Theory	245
12.1 Complexity of Arithmetic Computations	245
12.2 Public-key Cryptography	251
12.3 Primality Testing: Euclidean Algorithm	253
12.4 Primality Testing: Pseudoprimes	258
12.5 Carmichael Numbers	260
12.6 Probabilistic Primality Testing	262
12.7 The Agrawal–Kayal–Saxena Algorithm	266
12.8 Factorizing	269
12.9 Complexity of Arithmetic in Finite Fields	276
References	279
Index	287