

Contents

1	Introduction and Historical Remarks	1
2	Basic Number Theory	7
2.1	The Ring of Integers	7
2.2	Divisibility, Primes, and Composites	10
2.3	The Fundamental Theorem of Arithmetic	16
2.4	Congruences and Modular Arithmetic	22
2.4.1	Basic Theory of Congruences	22
2.4.2	The Ring of Integers Mod N	23
2.4.3	Units and the Euler Phi Function	27
2.4.4	Fermat's Little Theorem and the Order of an Element	32
2.4.5	On Cyclic Groups	36
2.5	The Solution of Polynomial Congruences Modulo m	39
2.5.1	Linear Congruences and the Chinese Remainder Theorem	39
2.5.2	Higher Degree Congruences	45
2.6	Quadratic Reciprocity	48
2.7	Exercises	55
3	The Infinitude of Primes	59
3.1	The Infinitude of Primes	59
3.1.1	Some Direct Proofs and Variations	59
3.1.2	Some Analytic Proofs and Variations	62
3.1.3	The Fermat and Mersenne Numbers	66
3.1.4	The Fibonacci Numbers and the Golden Section	71
3.1.5	Some Simple Cases of Dirichlet's Theorem	84
3.1.6	A Topological Proof and a Proof Using Codes	89
3.2	Sums of Squares	92
3.2.1	Pythagorean Triples	93
3.2.2	Fermat's Two-Square Theorem	96

3.2.3	The Modular Group	100
3.2.4	Lagrange's Four Square Theorem	107
3.2.5	The Infinitude of Primes Through Continued Fractions.	110
3.3	Dirichlet's Theorem	112
3.4	Twin Prime Conjecture and Related Ideas	131
3.5	Primes Between x and $2x$	132
3.6	Arithmetic Functions and the Möbius Inversion Formula	133
3.7	Exercises	138
4	The Density of Primes.	143
4.1	The Prime Number Theorem—Estimates and History	143
4.2	Chebyshev's Estimate and Some Consequences	147
4.3	Equivalent Formulations of the Prime Number Theorem	159
4.4	The Riemann Zeta Function and the Riemann Hypothesis	169
4.4.1	The Real Zeta Function of Euler.	170
4.4.2	Analytic Functions and Analytic Continuation	175
4.4.3	The Riemann Zeta Function	179
4.5	The Prime Number Theorem	186
4.6	The Elementary Proof.	193
4.7	Multiple Zeta Values	198
4.8	Some Extensions and Comments	206
4.9	Exercises	213
5	Primality Testing—An Overview	219
5.1	Primality Testing and Factorization	219
5.2	Sieving Methods.	220
5.2.1	Brun's Sieve and Brun's Theorem	226
5.3	Primality Testing and Prime Records	236
5.3.1	Pseudo-Primes and Probabilistic Testing.	241
5.3.2	The Lucas–Lehmer Test and Prime Records	249
5.3.3	Some Additional Primality Tests.	255
5.3.4	Elliptic Curve Methods	257
5.4	Cryptography and Primes	263
5.4.1	Some Number Theoretic Cryptosystems	267
5.5	Public Key Cryptography and the RSA Algorithm.	270
5.6	Elliptic Curve Cryptography	273
5.7	The AKS Algorithm.	276
5.8	Exercises	282
6	Primes and Algebraic Number Theory	285
6.1	Algebraic Number Theory	285
6.2	Unique Factorization Domains	287
6.2.1	Euclidean Domains and the Gaussian Integers	293
6.2.2	Principal Ideal Domains	301
6.2.3	Prime and Maximal Ideals	304

6.3	Algebraic Number Fields	308
6.3.1	Algebraic Extensions of \mathbb{Q}	316
6.3.2	Algebraic and Transcendental Numbers	319
6.3.3	Symmetric Polynomials.	321
6.3.4	Discriminant and Norm.	325
6.4	Algebraic Integers.	329
6.4.1	The Ring of Algebraic Integers.	331
6.4.2	Integral Bases	333
6.4.3	Quadratic Fields and Quadratic Integers	335
6.4.4	The Transcendence of e and π	339
6.4.5	The Geometry of Numbers—Minkowski Theory	342
6.4.6	Dirichlet's Unit Theorem	345
6.5	The Theory of Ideals	348
6.5.1	Unique Factorization of Ideals	350
6.5.2	An Application of Unique Factorization	357
6.5.3	The Ideal Class Group	359
6.5.4	Norms of Ideals	361
6.5.5	Class Number	364
6.6	Exercises	366
7	The Fields \mathbb{Q}_p of p-Adic Numbers: Hensel's Lemma	371
7.1	The p -Adic Fields and p -Adic Expansions	371
7.2	The Construction of the Real Numbers.	373
7.2.1	The Completeness of Real Numbers	373
7.2.2	The Construction of \mathbb{R}	376
7.2.3	The Characterization of \mathbb{R}	381
7.3	Normed Fields and Cauchy Completions	381
7.4	The p -Adic Fields.	382
7.4.1	The p -Adic Norm	385
7.5	The Construction of \mathbb{Q}_p	387
7.5.1	p -Adic Arithmetic and p -Adic Expansions	387
7.6	The p -Adic Integers	394
7.6.1	Principal Ideals and Unique Factorization	396
7.6.2	The Completeness of \mathbb{Z}_p	397
7.7	Ostrowski's Theorem	398
7.8	Hensel's Lemma and Applications	398
7.8.1	The Non-isomorphism of the p -Adic Fields	402
7.9	Exercises	403
	Bibliography	405
	Index	409

Number Theory

An Introduction via the Density of Primes

Fine, B.; Rosenberger, G.

2016, XIII, 413 p. 12 illus., 1 illus. in color., Hardcover

ISBN: 978-3-319-43873-3

A product of Birkhäuser Basel