
CONTENTS

Preface	xiii
Chapter 1. Introduction	1
1.1. Roots of Polynomials	2
1.2. Lines	5
1.3. Quadratic Equations and Conic Sections	7
1.4. Cubic Equations and Elliptic Curves	11
1.5. Curves of Higher Degree	14
1.6. Diophantine Equations	16
1.7. Hilbert's Tenth Problem	21
1.8. Exercises	23
Part 1. Integers, Polynomials, Lines, and Congruences	
Chapter 2. The Integers	29
2.1. The Axioms of \mathbb{Z}	29
2.2. Consequences of the Axioms	31
2.3. The Principle of Mathematical Induction	33
2.4. The Division Theorem	38
2.5. The Greatest Common Divisor	41
2.6. Euclid's Algorithm to Calculate a GCD	42
2.7. Bezout's Identity	43
2.8. Integral and Rational Roots of Polynomials	47
2.9. Integral and Rational Points in a Line	48
2.10. The Fundamental Theorem of Arithmetic	51
2.11. Exercises	55

Chapter 3. The Prime Numbers	61
3.1. The Sieve of Eratosthenes	62
3.2. The Infinitude of the Primes	63
3.3. Theorems on the Distribution of Primes	67
3.4. Famous Conjectures about Prime Numbers	72
3.5. Exercises	79
Chapter 4. Congruences	83
4.1. The Definition of Congruence	84
4.2. Basic Properties of Congruences	86
4.3. Cancellation Properties of Congruences	89
4.4. Linear Congruences	90
4.5. Systems of Linear Congruences	94
4.6. Applications	102
4.7. Exercises	113
Chapter 5. Groups, Rings, and Fields	119
5.1. $\mathbb{Z}/m\mathbb{Z}$	119
5.2. Groups	124
5.3. Rings	130
5.4. Fields	138
5.5. Rings of Polynomials	140
5.6. Exercises	149
Chapter 6. Finite Fields	155
6.1. An Example	155
6.2. Polynomial Congruences	156
6.3. Irreducible Polynomials	159
6.4. Fields with p^n Elements	160
6.5. Fields with p^2 Elements	161
6.6. Fields with s Elements	163
6.7. Exercises	164
Chapter 7. The Theorems of Wilson, Fermat, and Euler	167
7.1. Wilson's Theorem	167
7.2. Fermat's (Little) Theorem	170
7.3. Euler's Theorem	176
7.4. Euler's Phi Function	181
7.5. Applications	184
7.6. Exercises	188

Chapter 8. Primitive Roots	193
8.1. Multiplicative Order	195
8.2. Primitive Roots	200
8.3. Universal Exponents	203
8.4. Existence of Primitive Roots Modulo p	205
8.5. Primitive Roots Modulo p^k	210
8.6. Indices	214
8.7. Existence of Primitive Roots Modulo m	220
8.8. The Structure of $(\mathbb{Z}/p^k\mathbb{Z})^\times$	222
8.9. Applications	224
8.10. Exercises	230
 Part 2. Quadratic Congruences and Quadratic Equations	
Chapter 9. An Introduction to Quadratic Equations	237
9.1. Product of Two Lines	238
9.2. A Classification: Parabolas, Ellipses, and Hyperbolas	248
9.3. Rational Parametrizations of Conics	255
9.4. Integral Points on Quadratic Equations	260
9.5. Exercises	268
Chapter 10. Quadratic Congruences	271
10.1. The Quadratic Formula	272
10.2. Quadratic Residues	275
10.3. The Legendre Symbol	279
10.4. The Law of Quadratic Reciprocity	284
10.5. The Jacobi Symbol	290
10.6. Cipolla's Algorithm	296
10.7. Applications	298
10.8. Exercises	305
Chapter 11. The Hasse–Minkowski Theorem	309
11.1. Quadratic Forms	309
11.2. The Hasse–Minkowski Theorem	313
11.3. An Example of Hasse–Minkowski	318
11.4. Polynomial Congruences for Prime Powers	324
11.5. The p -Adic Numbers	328
11.6. Hensel's Lemma	331
11.7. Exercises	333

Chapter 12. Circles, Ellipses, and the Sum of Two Squares Problem	337
12.1. Rational and Integral Points on a Circle	337
12.2. Pythagorean Triples	343
12.3. Fermat's Last Theorem for $n = 4$	347
12.4. Ellipses	348
12.5. Quadratic Fields and Norms	350
12.6. Integral Points on Ellipses	353
12.7. Primes of the Form $X^2 + BY^2$	353
12.8. Exercises	356
Chapter 13. Continued Fractions	361
13.1. Finite Continued Fractions	363
13.2. Infinite Continued Fractions	370
13.3. Approximations of Irrational Numbers	386
13.4. Exercises	389
Chapter 14. Hyperbolas and Pell's Equation	393
14.1. Square Hyperbolas	393
14.2. Pell's Equation $x^2 - By^2 = 1$	395
14.3. Generalized Pell's Equations $x^2 - By^2 = N$	401
14.4. Exercises	409
Part 3. Cubic Equations and Elliptic Curves	
Chapter 15. An Introduction to Cubic Equations	413
15.1. The Projective Line and Projective Space	415
15.2. Singular Cubic Curves	422
15.3. Weierstrass Equations	425
15.4. Exercises	433
Chapter 16. Elliptic Curves	437
16.1. Definition	438
16.2. Integral Points	441
16.3. The Group Structure on $E(\mathbb{Q})$	441
16.4. The Torsion Subgroup	447
16.5. Elliptic Curves over Finite Fields	449
16.6. The Rank and the Free Part of $E(\mathbb{Q})$	455
16.7. Descent and the Weak Mordell–Weil Theorem	459
16.8. Homogeneous Spaces	467
16.9. Application: The Elliptic Curve Diffie–Hellman Key Exchange	471
16.10. Exercises	473

Bibliography	479
Index	483