

Contents

1	Modular Arithmetic	3
1.1	Sets, functions, numbers	3
1.2	Induction	14
1.3	Divisibility	19
1.4	Prime Numbers	26
1.5	Relations and Partitions	32
1.6	Modular Arithmetic	36
1.7	Equations in $\mathbb{Z}_n$	44
1.8	Bar codes	51
1.9	The Chinese Remainder Theorem	56
1.10	Euler's function	61
1.11	Theorems of Euler and Fermat	64
1.12	Public Key Cryptosystems	68
2	Rings and Fields	79
2.1	Basic Properties	79
2.2	Subrings and Subfields	86
2.3	Review of Vector Spaces	95
2.4	Polynomials	100
2.5	Polynomial Evaluation and Interpolation	109
2.6	Irreducible Polynomials	116
2.7	Construction of Fields	123
2.8	Extension Fields	130
2.9	Multiplicative Structure of Finite Fields	140

2.10	Primitive Elements	143
2.11	Subfield Structure of Finite Fields	148
2.12	Minimal Polynomials	152
2.13	Isomorphisms between Fields	161
2.14	Error Correcting Codes	168
3	Groups and Permutations	181
3.1	Basic Properties	181
3.2	Subgroups	193
3.3	Permutation Groups	200
3.4	Matrix Groups	207
3.5	Even and Odd Permutations	213
3.6	Cayley's Theorem	217
3.7	Lagrange's Theorem	220
3.8	Orbits	228
3.9	Orbit/Stabilizer Theorem	234
3.10	The Cauchy-Frobenius Theorem	241
3.11	K-Colorings	250
3.12	Cycle Index and Enumeration	254
4	Groups: Homomorphisms and Subgroups	264
4.1	Homomorphisms	264
4.2	The Isomorphism Theorems	274
4.3	Direct Products	278
4.4	Finite Abelian Groups	283
4.5	Conjugacy and the Class Equation	292
4.6	The Sylow Theorems 1 and 2	299
4.7	Sylow's Third Theorem	305
4.8	Solvable Groups	309
4.9	Nilpotent Groups	315
4.10	The Enigma Encryption Machine	322
5	Rings and Polynomials	331
5.1	Homomorphisms and Ideals	331
5.2	Polynomial Rings	339
5.3	Division Algorithm in $F[x_1, x_2, \dots, x_n]$: Single Divisor	349
5.4	Multiple Divisors: Groebner Bases	358
5.5	Ideals and Affine Varieties	367
5.6	Decomposition of Affine Varieties	376
5.7	Cubic Equations in One Variable	381
5.8	Parameters	383
5.9	Intersection Multiplicities	394
5.10	Singular and Nonsingular Points	399
6	Elliptic Curves	403
6.1	Elliptic Curves	403
6.2	Homogeneous Polynomials	408

6.3	Projective Space	414
6.4	Intersection of Lines and Curves	427
6.5	Defining Curves by Points	433
6.6	Classification of Conics	439
6.7	Reducible Conics and Cubics	443
6.8	The Nine-Point Theorem	447
6.9	Groups on Elliptic Curves	453
6.10	The Arithmetic on an Elliptic Curve	458
6.11	Results Concerning the Structure of Groups on Elliptic Curves	466
7	Further Topics Related to Elliptic Curves	471
7.1	Elliptic Curve Cryptosystems	471
7.2	Fermat's Last Theorem	475
7.3	Elliptic Curve Factoring Algorithm	480
7.4	Singular Curves of Form $y^2 = x^3 + ax + b$	485
7.5	Birational Equivalence	488
7.6	The Genus of a Curve	494
7.7	Pell's Equation	496
	References	503
	Index	505