

Contents

Preface	v
Introduction	1
CHAPTER I	
Algebraic Varieties	5
§1. Affine Varieties	5
§2. Projective Varieties	10
§3. Maps between Varieties	15
CHAPTER II	
Algebraic Curves	21
§1. Curves	21
§2. Maps between Curves	23
§3. Divisors	31
§4. Differentials	34
§5. The Riemann–Roch Theorem	37
CHAPTER III	
The Geometry of Elliptic Curves	45
§1. Weierstrass Equations	46
§2. The Group Law	55
§3. Elliptic Curves	63
§4. Isogenies	70
§5. The Invariant Differential	79

§6. The Dual Isogeny	84
§7. The Tate Module	90
§8. The Weil Pairing	95
§9. The Endomorphism Ring	100
§10. The Automorphism Group	103
CHAPTER IV	
The Formal Group of an Elliptic Curve	110
§1. Expansion around O	110
§2. Formal Groups	115
§3. Groups Associated to Formal Groups	117
§4. The Invariant Differential	119
§5. The Formal Logarithm	121
§6. Formal Groups over Discrete Valuation Rings	123
§7. Formal Groups in Characteristic p	126
CHAPTER V	
Elliptic Curves over Finite Fields	130
§1. Number of Rational Points	130
§2. The Weil Conjectures	132
§3. The Endomorphism Ring	137
§4. Calculating the Hasse Invariant	140
CHAPTER VI	
Elliptic Curves over \mathbb{C}	146
§1. Elliptic Integrals	147
§2. Elliptic Functions	150
§3. Construction of Elliptic Functions	153
§4. Maps—Analytic and Algebraic	159
§5. Uniformization	161
§6. The Lefschetz Principle	164
CHAPTER VII	
Elliptic Curves over Local Fields	171
§1. Minimal Weierstrass Equations	171
§2. Reduction Modulo π	173
§3. Points of Finite Order	175
§4. The Action of Inertia	178
§5. Good and Bad Reduction	179
§6. The Group E/E_0	183
§7. The Criterion of Néron—Ogg—Shafarevich	184

CHAPTER VIII	189
Elliptic Curves over Global Fields	190
§1. The Weak Mordell–Weil Theorem	196
§2. The Kummer Pairing via Cohomology	199
§3. The Descent Procedure	201
§4. The Mordell–Weil Theorem over \mathbb{Q}	205
§5. Heights on Projective Space	215
§6. Heights on Elliptic Curves	220
§7. Torsion Points	223
§8. The Minimal Discriminant	227
§9. The Canonical Height	233
§10. The Rank of an Elliptic Curve	
 CHAPTER IX	
Integral Points on Elliptic Curves	241
§1. Diophantine Approximation	242
§2. Distance Functions	245
§3. Siegel’s Theorem	247
§4. The S -Unit Equation	252
§5. Effective Methods	256
§6. Shafarevich’s Theorem	263
§7. The Curve $Y^2 = X^3 + D$	266
§8. Roth’s Theorem—An Overview	269
 CHAPTER X	
Computing the Mordell–Weil Group	276
§1. An Example	277
§2. Twisting—General Theory	284
§3. Homogeneous Spaces	287
§4. The Selmer and Shafarevich–Tate Groups	296
§5. Twisting—Elliptic Curves	306
§6. The Curve $Y^2 = X^3 + DX$	309
 APPENDIX A	
Elliptic Curves in Characteristics 2 and 3	324
 APPENDIX B	
Group Cohomology (H^0 and H^1)	330
§1. Cohomology of Finite Groups	330
§2. Galois Cohomology	333
§3. Non-Abelian Cohomology	335

APPENDIX C	
Further Topics: An Overview	338
§11. Complex Multiplication	338
§12. Modular Functions	342
§13. Modular Curves	351
§14. Tate Curves	355
§15. Néron Models and Tate's Algorithm	357
§16. L -Series	360
§17. Duality Theory	364
§18. Local Height Functions	364
§19. The Image of Galois	366
§20. Function Fields and Specialization Theorems	367
Notes on Exercises	369
Bibliography	372
List of Notation	379
Index	385