## Contents

Preface to the Second Edition

Preface to the First Edition

Introduction

CHAPTER I
Algebraic Varieties 1
  §1. Affine Varieties 1
  §2. Projective Varieties 6
  §3. Maps Between Varieties 11
    Exercises 14

CHAPTER II
Algebraic Curves 17
  §1. Curves 17
  §2. Maps Between Curves 19
  §3. Divisors 27
  §4. Differentials 30
  §5. The Riemann–Roch Theorem 33
    Exercises 37

CHAPTER III
The Geometry of Elliptic Curves 41
  §1. Weierstrass Equations 42
  §2. The Group Law 51
  §3. Elliptic Curves 58
  §4. Isogenies 66
  §5. The Invariant Differential 75
§6. The Dual Isogeny 80
§7. The Tate Module 87
§8. The Weil Pairing 92
§9. The Endomorphism Ring 99
§10. The Automorphism Group 103
Exercises 104

CHAPTER IV
The Formal Group of an Elliptic Curve 115
§1. Expansion Around $O$ 115
§2. Formal Groups 120
§3. Groups Associated to Formal Groups 123
§4. The Invariant Differential 125
§5. The Formal Logarithm 127
§6. Formal Groups over Discrete Valuation Rings 129
§7. Formal Groups in Characteristic $p$ 132
Exercises 135

CHAPTER V
Elliptic Curves over Finite Fields 137
§1. Number of Rational Points 137
§2. The Weil Conjectures 140
§3. The Endomorphism Ring 144
§4. Calculating the Hasse Invariant 148
Exercises 153

CHAPTER VI
Elliptic Curves over $\mathbb{C}$ 157
§1. Elliptic Integrals 158
§2. Elliptic Functions 161
§3. Construction of Elliptic Functions 165
§4. Maps Analytic and Maps Algebraic 171
§5. Uniformization 173
§6. The Lefschetz Principle 177
Exercises 178
CHAPTER VII
Elliptic Curves over Local Fields

§1. Minimal Weierstrass Equations 185
§2. Reduction Modulo $\pi$ 187
§3. Points of Finite Order 192
§4. The Action of Inertia 194
§5. Good and Bad Reduction 196
§6. The Group $E/E_0$ 199
§7. The Criterion of Néron–Ogg–Shafarevich 201
Exercises 203

CHAPTER VIII
Elliptic Curves over Global Fields

§1. The Weak Mordell–Weil Theorem 208
§2. The Kummer Pairing via Cohomology 215
§3. The Descent Procedure 218
§4. The Mordell–Weil Theorem over $\mathbb{Q}$ 220
§5. Heights on Projective Space 224
§6. Heights on Elliptic Curves 234
§7. Torsion Points 240
§8. The Minimal Discriminant 243
§9. The Canonical Height 247
§10. The Rank of an Elliptic Curve 254
§11. Szpiro’s Conjecture and $ABC$ 255
Exercises 261

CHAPTER IX
Integral Points on Elliptic Curves

§1. Diophantine Approximation 270
§2. Distance Functions 273
§3. Siegel’s Theorem 276
§4. The $S$-Unit Equation 281
§5. Effective Methods 286
§6. Shafarevich’s Theorem 293
§7. The Curve $Y^2 = X^3 + D$ 296
§8. Roth’s Theorem—An Overview 299
Exercises 302
APPENDIX C

Further Topics: An Overview 425

§11. Complex Multiplication 425
§12. Modular Functions 429
§13. Modular Curves 439
§14. Tate Curves 443
§15. Néron Models and Tate’s Algorithm 446
§16. L-Series 449
§17. Duality Theory 453
§18. Local Height Functions 454
§19. The Image of Galois 455
§20. Function Fields and Specialization Theorems 456
§21. Variation of $\alpha_p$ and the Sato–Tate Conjecture 458

Notes on Exercises 461

List of Notation 467

References 473

Index 489
The Arithmetic of Elliptic Curves
Silverman, J.H.
2009, XX, 513 p. 14 illus., Hardcover