

Contents

Preface	v
Introduction	xv
1 Geometry and Arithmetic	1
1.1 Rational Points on Conics	1
1.2 The Geometry of Cubic Curves	8
1.3 Weierstrass Normal Form	16
1.4 Explicit Formulas for the Group Law	23
Exercises	28
2 Points of Finite Order	35
2.1 Points of Order Two and Three	35
2.2 Real and Complex Points on Cubic Curves	38
2.3 The Discriminant	45
2.4 Points of Finite Order Have Integer Coordinates	47
2.5 The Nagell–Lutz Theorem and Further Developments	56
Exercises	58
3 The Group of Rational Points	65
3.1 Heights and Descent	65
3.2 The Height of $P + P_0$	71
3.3 The Height of $2P$	75
3.4 A Useful Homomorphism	80
3.5 Mordell’s Theorem	88

Examples and Further Developments	95
3.7 Singular Cubic Curves	106
Exercises	111
4 Cubic Curves over Finite Fields	117
4.1 Rational Points over Finite Fields	117
4.2 A Theorem of Gauss	121
4.3 Points of Finite Order Revisited	133
4.4 A Factorization Algorithm Using Elliptic Curves	139
4.5 Elliptic Curve Cryptography	152
Exercises	157
5 Integer Points on Cubic Curves	167
5.1 How Many Integer Points?	167
5.2 Taxicabs and Sums of Two Cubes	170
5.3 Thue's Theorem and Diophantine Approximation	176
5.4 Construction of an Auxiliary Polynomial	182
5.5 The Auxiliary Polynomial Is Small	190
5.6 The Auxiliary Polynomial Does Not Vanish	193
5.7 Proof of the Diophantine Approximation Theorem	197
5.8 Further Developments	200
Exercises	202
6 Complex Multiplication	207
6.1 Abelian Extensions of $\mathbb{Q}$	207
6.2 Algebraic Points on Cubic Curves	213
6.3 A Galois Representation	221
6.4 Complex Multiplication	230
6.5 Abelian Extensions of $\mathbb{Q}(i)$	235
6.6 Elliptic Curves and Fermat's Last Theorem	245
Exercises	256
A Projective Geometry	265
A.1 Homogeneous Coordinates and the Projective Plane	265
A.2 Curves in the Projective Plane	271
A.3 Intersections of Projective Curves	280

A.4 Intersection Multiplicities and a Proof of Bezout's Theorem	290
A.5 Reduction Modulo p	302
Exercises	305

B Transformation to Weierstrass Form	311
---	------------

List of Notation	315
-----------------------------------	------------

References	317
-----------------------------	------------

Index	323
------------------------	------------