

Contents

Basic Tools

Preface	xi
Preface to the English Edition	xvii
Chapter 0. Synopsis	1
0.1. Simple paraphrase	1
0.2. Elliptic curves	3
0.3. Elliptic curves and modular forms	5
0.4. Conductor of an elliptic curve and level of a modular form	7
0.5. ℓ -torsion points of elliptic curves and modular forms	9
Chapter 1. Elliptic curves	13
1.1. Elliptic curves over a field	13
1.2. Reduction mod p	15
1.3. Morphisms and the Tate modules	22
1.4. Elliptic curves over an arbitrary scheme	26
1.5. Generalized elliptic curves	29
Chapter 2. Modular forms	35
2.1. The j -invariant	35
2.2. Moduli spaces	37
2.3. Modular curves and modular forms	40
2.4. Construction of modular curves	44
2.5. The genus formula	52
2.6. The Hecke operators	55
2.7. The q -expansions	58
2.8. Primary forms, primitive forms	62
2.9. Elliptic curves and modular forms	65

2.10.	Primary forms, primitive forms, and Hecke algebras	66
2.11.	The analytic expression	70
2.12.	The q -expansion and analytic expression	74
2.13.	The q -expansion and Hecke operators	77
Chapter 3.	Galois representations	81
3.1.	Frobenius substitutions	82
3.2.	Galois representations and finite group schemes	86
3.3.	The Tate module of an elliptic curve	89
3.4.	Modular ℓ -adic representations	91
3.5.	Ramification conditions	96
3.6.	Finite flat group schemes	100
3.7.	Ramification of the Tate module of an elliptic curve	103
3.8.	Level of modular forms and ramification	108
Chapter 4.	The 3–5 trick	111
4.1.	Proof of Theorem 2.54	111
4.2.	Summary of the Proof of Theorem 0.1	116
Chapter 5.	$R = T$	119
5.1.	What is $R = T$?	119
5.2.	Deformation rings	122
5.3.	Hecke algebras	126
5.4.	Some commutative algebra	131
5.5.	Hecke modules	135
5.6.	Outline of the Proof of Theorem 5.22	137
Chapter 6.	Commutative algebra	143
6.1.	Proof of Theorem 5.25	143
6.2.	Proof of Theorem 5.27	149
Chapter 7.	Deformation rings	159
7.1.	Functors and their representations	159
7.2.	The existence theorem	161
7.3.	Proof of Theorem 5.8	162
7.4.	Proof of Theorem 7.7	166
Appendix A.	Supplements to scheme theory	171
A.1.	Various properties of schemes	171
A.2.	Group schemes	175
A.3.	Quotient by a finite group	177
A.4.	Flat covering	178

A.5. G -torsor	179
A.6. Closed condition	182
A.7. Cartier divisor	183
A.8. Smooth commutative group scheme	185
Bibliography	189
Symbol Index	197
Subject Index	199

The Proof

Preface	ix
Preface to the English Edition	xv
Chapter 8. Modular curves over \mathbf{Z}	1
8.1. Elliptic curves in characteristic $p > 0$	1
8.2. Cyclic group schemes	6
8.3. Drinfeld level structure	12
8.4. Modular curves over \mathbf{Z}	20
8.5. Modular curve $Y(r)_{\mathbf{Z}[\frac{1}{r}]}$	25
8.6. Igusa curves	32
8.7. Modular curve $Y_1(N)_{\mathbf{Z}}$	37
8.8. Modular curve $Y_0(N)_{\mathbf{Z}}$	41
8.9. Compactifications	48
Chapter 9. Modular forms and Galois representations	61
9.1. Hecke algebras with \mathbf{Z} coefficients	61
9.2. Congruence relations	70
9.3. Modular mod ℓ representations and non-Eisenstein ideals	76
9.4. Level of modular forms and ramification of ℓ -adic representations	81
9.5. Old part	90
9.6. Néron model of the Jacobian $J_0(Mp)$	97
9.7. Level of modular forms and ramification of mod ℓ representations	102

Chapter 10. Hecke modules	107
10.1. Full Hecke algebras	108
10.2. Hecke modules	113
10.3. Proof of Proposition 10.11	118
10.4. Deformation rings and group rings	125
10.5. Family of liftings	129
10.6. Proof of Proposition 10.37	136
10.7. Proof of Theorem 5.22	140
Chapter 11. Selmer groups	143
11.1. Cohomology of groups	143
11.2. Galois cohomology	149
11.3. Selmer groups	157
11.4. Selmer groups and deformation rings	161
11.5. Calculation of local conditions and proof of Proposition 11.38	165
11.6. Proof of Theorem 11.37	169
Appendix B. Curves over discrete valuation rings	179
B.1. Curves	179
B.2. Semistable curve over a discrete valuation ring	182
B.3. Dual chain complex of curves over a discrete valuation ring	187
Appendix C. Finite commutative group scheme over \mathbf{Z}_p	191
C.1. Finite flat commutative group scheme over \mathbf{F}_p	191
C.2. Finite flat commutative group scheme over \mathbf{Z}_p	192
Appendix D. Jacobian of a curve and its Néron model	199
D.1. The divisor class group of a curve	199
D.2. The Jacobian of a curve	201
D.3. The Néron model of an abelian variety	205
D.4. The Néron model of the Jacobian of a curve	209
Bibliography	213
Symbol Index	217
Subject Index	221