

Contents

Preface	v
Contributors	xiii
Schedule of Lectures	xvii
Introduction	xix

CHAPTER I

An Overview of the Proof of Fermat's Last Theorem

GLENN STEVENS

§1. A remarkable elliptic curve	2
§2. Galois representations	3
§3. A remarkable Galois representation	7
§4. Modular Galois representations	7
§5. The Modularity Conjecture and Wiles's Theorem	9
§6. The proof of Fermat's Last Theorem	10
§7. The proof of Wiles's Theorem	10
References	15

CHAPTER II

A Survey of the Arithmetic Theory of Elliptic Curves

JOSEPH H. SILVERMAN

§1. Basic definitions	17
§2. The group law	18
§3. Singular cubics	18
§4. Isogenies	19
§5. The endomorphism ring	19
§6. Torsion points	20
§7. Galois representations attached to E	20
§8. The Weil pairing	21
§9. Elliptic curves over finite fields	22
§10. Elliptic curves over \mathbb{C} and elliptic functions	24
§11. The formal group of an elliptic curve	26
§12. Elliptic curves over local fields	27
§13. The Selmer and Shafarevich-Tate groups	29
§14. Discriminants, conductors, and L -series	31
§15. Duality theory	33

§16. Rational torsion and the image of Galois	34
§17. Tate curves	34
§18. Heights and descent	35
§19. The conjecture of Birch and Swinnerton-Dyer	37
§20. Complex multiplication	37
§21. Integral points	39
References	40

CHAPTER III

41

Modular Curves, Hecke Correspondences, and L -Functions

DAVID E. ROHRLICH

§1. Modular curves	41
§2. The Hecke correspondences	61
§3. L -functions	73
References	99

CHAPTER IV

101

Galois Cohomology

LAWRENCE C. WASHINGTON

§1. H^0 , H^1 , and H^2	101
§2. Preliminary results	105
§3. Local Tate duality	107
§4. Extensions and deformations	108
§5. Generalized Selmer groups	111
§6. Local conditions	113
§7. Conditions at p	114
§8. Proof of theorem 2	117
References	120

CHAPTER V

121

Finite Flat Group Schemes

JOHN TATE

Introduction 121

§1. Group objects in a category	122
§2. Group schemes. Examples	125
§3. Finite flat group schemes; passage to quotient	132
§4. Raynaud's results on commutative p -group schemes	146
References	154

CHAPTER VI

155

Three Lectures on the Modularity of $\bar{\rho}_{E,3}$
and the Langlands Reciprocity Conjecture

STEPHEN GELBART

Lecture I. The modularity of $\bar{\rho}_{E,3}$ and automorphic representations
of weight one 156

§1. The modularity of $\bar{\rho}_{E,3}$	157
§2. Automorphic representations of weight one	164
Lecture II. The Langlands program: Some results and methods	
§3. The local Langlands correspondence for $GL(2)$	176
§4. The Langlands reciprocity conjecture (LRC)	179
§5. The Langlands functoriality principle theory and results	182

Lecture III. Proof of the Langlands-Tunnell theorem	192
§6. Base change theory	192
§7. Application to Artin's conjecture	197
References	204

CHAPTER VII

209

Serre's Conjectures

BAS EDIXHOVEN

§1. Serre's conjecture: statement and results	209
§2. The cases we need	222
§3. Weight two, trivial character and square free level	224
§4. Dealing with the Langlands-Tunnell form	230
References	239

CHAPTER VIII

243

An Introduction to the Deformation Theory of
Galois Representations

BARRY MAZUR

Chapter I. Galois representations	246
Chapter II. Group representations	251
Chapter III. The deformation theory for Galois representations	259
Chapter IV. Functors and representability	267
Chapter V. Zariski tangent spaces and deformation problems subject to "conditions"	284
Chapter VI. Back to Galois representations	294
References	309

CHAPTER IX

313

Explicit Construction of Universal Deformation Rings

BART DE SMIT AND HENDRIK W. LENSTRA, JR.

§1. Introduction	313
§2. Main results	314
§3. Lifting homomorphisms to matrix groups	317
§4. The condition of absolute irreducibility	318
§5. Projective limits	320
§6. Restrictions on deformations	323
§7. Relaxing the absolute irreducibility condition	324
References	326

CHAPTER X

327

Hecke Algebras and the Gorenstein Property

JACQUES TILOUINE

§1. The Gorenstein property	328
§2. Hecke algebras	330
§3. The main theorem	331
§4. Strategy of the proof of theorem 3.4	334
§5. Sketch of the proof	335
Appendix	340
References	341

	CHAPTER XI	343
Criteria for Complete Intersections		
BART DE SMIT, KARL RUBIN, AND RENÉ SCHOOF		
Introduction	343	
§1. Preliminaries	345	
§2. Complete intersections	347	
§3. Proof of Criterion I	350	
§4. Proof of Criterion II	353	
Bibliography	355	
	CHAPTER XII	357
ℓ -adic Modular Deformations and Wiles's "Main Conjecture"		
FRED DIAMOND AND KENNETH A. RIBET		
§1. Introduction	357	
§2. Strategy	358	
§3. The "Main Conjecture"	359	
§4. Reduction to the case $\Sigma = \emptyset$	363	
§5. Epilogue	370	
Bibliography	370	
	CHAPTER XIII	373
The Flat Deformation Functor		
BRIAN CONRAD		
Introduction	373	
§0. Notation	374	
§1. Motivation and flat representations	375	
§2. Defining the functor	394	
§3. Local Galois cohomology and deformation theory	397	
§4. Fontaine's approach to finite flat group schemes	406	
§5. Applications to flat deformations	412	
References	418	
	CHAPTER XIV	421
Hecke Rings and Universal Deformation Rings		
EHUD DE SHALIT		
§1. Introduction	421	
§2. An outline of the proof	424	
§3. Proof of proposition 10 – On the structure of the Hecke algebra	432	
§4. Proof of proposition 11 – On the structure of the universal deformation ring	436	
§5. Conclusion of the proof: Some group theory	442	
Bibliography	444	
	CHAPTER XV	447
Explicit Families of Elliptic Curves		
with Prescribed Mod N Representations		
ALICE SILVERBERG		
Introduction	447	
Part 1. Elliptic curves with the same mod N representation	448	
§1. Modular curves and elliptic modular surfaces of level N	448	
§2. Twists of Y_N and W_N	449	
§3. Model for W when $N = 3, 4$, or 5	450	
§4. Level 4	451	

Part 2. Explicit families of modular elliptic curves 454

§5. Modular j invariants 454

§6. Semistable reduction 455

§7. Mod 4 representations 456

§8. Torsion subgroups 457

References 461

CHAPTER XVI

463

Modularity of Mod 5 Representations

KARL RUBIN

Introduction 463

§1. Preliminaries: Group theory 465

§2. Preliminaries: Modular curves 466

§3. Proof of the irreducibility theorem (Theorem 1) 470

§4. Proof of the modularity theorem (Theorem 2) 470

§5. Mod 5 representations and elliptic curves 471

References 473

CHAPTER XVII

475

An Extension of Wiles' Results

FRED DIAMOND

§1. Introduction 475

§2. Local representations mod ℓ 476

§3. Minimally ramified liftings 480

§4. Universal deformation rings 481

§5. Hecke algebras 482

§6. The main results 483

§7. Sketch of proof 484

References 488

APPENDIX TO CHAPTER XVII

491

Classification of $\overline{\rho}_{E,\ell}$ by the j Invariant of E

FRED DIAMOND AND KENNETH KRAMER

CHAPTER XVIII

499

Class Field Theory and the First Case of Fermat's Last Theorem

HENDRIK W. LENSTRA, JR. AND PETER STEVENHAGEN

CHAPTER XIX

505

Remarks on the History of Fermat's Last Theorem 1844 to 1984

MICHAEL ROSEN

Introduction 507

§1. Fermat's last theorem for polynomials 507

§2. Kummer's work on cyclotomic fields 508

§3. Fermat's last theorem for regular primes and certain other cases 513

§4. The structure of the p -class group 517

§5. Suggested readings 521

Appendix A: Kummer congruence and Hilbert's theorem 94 522

Bibliography 524

CHAPTER XX	527
On Ternary Equations of Fermat Type and Relations with Elliptic Curves	
GERHARD FREY	
§1. Conjectures	527
§2. The generic case	540
§3. $K = \mathbf{Q}$	542
References	548
CHAPTER XXI	549
Wiles' Theorem and the Arithmetic of Elliptic Curves	
HENRI DARMON	
§1. Prelude: plane conics, Fermat and Gauss	549
§2. Elliptic curves and Wiles' theorem	552
§3. The special values of $L(E/\mathbf{Q}, s)$ at $s = 1$	557
§4. The Birch and Swinnerton-Dyer conjecture	563
References	566
Index	573