

Gary Cornell
Joseph H. Silverman
Glenn Stevens
Editors

Modular Forms and Fermat's Last Theorem

模形式与费马大定理



Springer

世界图书出版公司
www.wpcbj.com.cn

Gary Cornell
Joseph H. Silverman
Glenn Stevens
Editors

Modular Forms and Fermat's Last Theorem

ISSN 1430-2655 (print) / 1430-2663 (electronic)



Springer

Volume 17 Number 1 2014
www.springer.com/MLM

Gary Cornell Joseph H. Silverman
Glenn Stevens

Editors

Modular Forms and Fermat's Last Theorem



Springer

图书在版编目 (CIP) 数据

模形式与费马大定理 = Modular forms and fermat's last theorem; 英文/(美) 康奈尔 (Cornell, G.) 著. —影印本. —北京: 世界图书出版公司北京公司, 2013. 10
ISBN 978 - 7 - 5100 - 7017 - 4

I. ①模… II. ①康… III. ①费马大定理—研究—英文 IV. ①O156

中国版本图书馆 CIP 数据核字 (2013) 第 249213 号

书 名: Modular Forms and Fermat's Last Theorem
作 者: Gary Cornell, Joseph H. Silverman, Glenn Stevens
中译名: 模形式与费马大定理
责任编辑: 高蓉 刘慧

出 版 者: 世界图书出版公司北京公司
印 刷 者: 三河市国英印务有限公司
发 行 者: 世界图书出版公司北京公司 (北京朝内大街 137 号 100010)
联系电话: 010 - 64021602, 010 - 64015659
电子信箱: kjb@wpcbj.com.cn

开 本: 24 开
印 张: 25.5
版 次: 2014 年 3 月
版权登记: 图字: 01 - 2013 - 2918

书 号: 978 - 7 - 5100 - 7017 - 4 定 价: 89.00 元

Gary Cornell
Department of Mathematics
University of Connecticut
Storrs, CT 06268
USA

Joseph H. Silverman
Department of Mathematics
Brown University
Providence, RI 02912
USA

Glenn Stevens
Department of Mathematics
Boston University
Boston, MA 02215
USA

Mathematics Subject Classification (1991): 11D41, 11G18, 14Hxx, 11-03

Library of Congress Cataloging-in-Publication Data

Modular forms and Fermat's last theorem / edited by Gary Cornell,
Joseph H. Silverman, Glenn Stevens ; with contributions by B. Conrad
[et al.].

p. cm.

Papers from a conference held Aug. 9-18, 1995, at Boston

University

Includes bibliographical references and index.

ISBN 0-387-98998-6 (alk. paper)

1. Curves, Elliptic—Congresses. 2. Forms, Modular—Congresses.

3. Fermat's last theorem—Congresses. I. Cornell Gary.

II. Silverman, Joseph H., 1955- . III. Stevens, Glenn, 1953- .

QA567.2.E44M63 1997

512'.74—dc21

97-10930

© 1997 Springer-Verlag New York, Inc.

All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer-Verlag New York, Inc., 175 Fifth Avenue, New York, NY 10010, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden.

The use of general descriptive names, trade names, trademarks, etc., in this publication, even if the former are not especially identified, is not to be taken as a sign that such names, as understood by the Trade Marks and Merchandise Marks Act, may accordingly be used freely by anyone.

Reprint from English language edition:

Modular Forms and Fermat's Last Theorem

by Gary Cornell, Joseph H. Silverman, Glenn Stevens

Copyright © 1997, Springer-Verlag New York, Inc.

Springer-Verlag New York is a part of Springer Science+Business Media

All Rights Reserved

This reprint has been authorized by Springer Science & Business Media for distribution in China Mainland only and not for export therefrom.

Preface

This volume is the record of an instructional conference on number theory and arithmetic geometry held from August 9 through 18, 1995 at Boston University. It contains expanded versions of all of the major lectures given during the conference. We want to thank all of the speakers, all of the writers whose contributions make up this volume, and all of the “behind-the-scenes” folks whose assistance was indispensable in running the conference. We would especially like to express our appreciation to Patricia Pacelli, who coordinated most of the details of the conference while in the midst of writing her PhD thesis, to Jaap Top and Jerry Tunnell, who stepped into the breach on short notice when two of the invited speakers were unavoidably unable to attend, and to Stephen Gelbart, whose courage and enthusiasm in the face of adversity has been an inspiration to us.

Finally, the conference was only made possible through the generous support of Boston University, the Vaughn Foundation, the National Security Agency and the National Science Foundation. In particular, their generosity allowed us to invite a multitude of young mathematicians, making the BU conference one of the largest and liveliest number theory conferences ever held.

January 13, 1997

G. Cornell
J.H. Silverman
G. Stevens

Contributors and Speakers

BRIAN CONRAD

Department of Mathematics, Harvard University, One Oxford Street,
Cambridge, MA 02138 USA.
(bconrad@math.harvard.edu)

GARY CORNELL

Department of Mathematics, University of Connecticut at Storrs,
Storrs, CT 06269 USA.
(gcornell@nsf.gov)

HENRI DARMON

Department of Mathematics, McGill University, Montréal, Québec,
H3A-2K6 Canada.
(darmon@math.mcgill.ca, www.math.mcgill.ca/~darmon)

EHUD DE SHALIT

Institute of Mathematics, Hebrew University, Giv'at-Ram, 91904 Jeru-
salem Israel.
(deshalit@math.huji.ac.il)

BART DE SMIT

Vakgroep Wiskunde, Universiteit van Amsterdam, Plantage Muider-
gracht 24, 1018 TV Amsterdam, The Netherlands.
(bds@wins.uva.nl)

FRED DIAMOND

Department of Mathematics, Massachusetts Institute of Technology,
77 Massachusetts Avenue, Cambridge, MA 02139 USA.
(fdiamond@math.mit.edu)

BAS EDIXHOVEN

Institut Mathématique, Université de Rennes 1, Campus de Beaulieu,
35042 Rennes cedex France.
(edix@univ-rennes1.fr)

GERHARD FREY

Institute for Experimental Mathematics, University of Essen, 29, El-
lernstrasse, 45326 Essen Germany.
(frey@exp-math.uni-essen.de)

STEPHEN GELBART

Department of Mathematics, Weizmann Institute of Science, Rehovot
76100 Israel.
(gelbar@wisdom.weizmann.ac.il)

BENEDICT H. GROSS

Department of Mathematics, Harvard University, One Oxford Street,
Cambridge, MA 02138 USA.
(gross@math.harvard.edu)

KENNETH KRAMER

Department of Mathematics, Queens College, City University of New
York, 65-30 Kissena Boulevard, Flushing, NY 11367 USA.
(kramer@qcvcaxa.acc.qc.edu)

HENDRIK W. LENSTRA, JR.

Department of Mathematics 3840, University of California, Berkeley,
CA 94720 3840 USA.
(hwl@math.berkeley.edu)

BARRY MAZUR

Department of Mathematics, 1 Oxford Street, 325 Science Center, Har-
vard University, Cambridge, MA 02138 USA.
(mazur@math.harvard.edu)

KENNETH A. RIBET

Department of Mathematics 3840, University of California, Berkeley,
CA 94720 USA.
(ribet@math.berkeley.edu)

DAVID E. ROHRLICH

Department of Mathematics, Boston University, 111 Cummington
Street, Boston, MA 02215 USA.
(rohrlich@math.bu.edu)

MICHAEL ROSEN

Department of Mathematics, Box 1917, Brown University, Providence,
RI 02912 USA.
(michael_rosen@brown.edu)

KARL RUBIN

Department of Mathematics, Ohio State University, 231 W. 18th Avenue, Columbus, OH 43210 USA.

(rubin@math.ohio-state.edu, www.math.ohio-state.edu/~rubin)

RENÉ SCHOOF

2^a Università di Roma "Tor Vergata", Dipartimento di Matematica, I-00133 Roma Italy.

(schoof@fwi.uva.nl)

ALICE SILVERBERG

Department of Mathematics, Ohio State University, 231 W. 18 Avenue, Columbus, OH 43210 USA.

(silver@math.ohio-state.edu)

JOSEPH H. SILVERMAN

Department of Mathematics, Box 1917, Brown University, Providence, RI 02912 USA.

(jhs@gauss.math.brown.edu, www.math.brown.edu/~jhs)

PETER STEVENHAGEN

Faculteit WINS, Universiteit van Amsterdam, Plantage Muidergracht 24, 1018 TV Amsterdam, The Netherlands.

(psh@wins.uva.nl)

GLENN STEVENS

Department of Mathematics, Boston University, 111 Cummington Street, Boston, MA 02215 USA.

(ghs@math.bu.edu)

JOHN TATE

Department of Mathematics, University of Texas at Austin, Austin, TX 78712 USA.

(tate@math.utexas.edu)

JACQUES TILOUINE

Département de Mathématiques, UA742, Université de Paris-Nord, 93430 Villetaneuse France.

(tilouine@math.univ-paris13.fr)

JAAP TOP

Vakgroep Wiskunde RuG, P.O. Box 800, 9700 AV Groningen, The Netherlands.

(top@math.rug.nl)

JERRY TUNNELL

Department of Mathematics, Rutgers University, New Brunswick, NJ 08903 USA.

(tunnell@math.rutgers.edu)

LAWRENCE C. WASHINGTON

Department of Mathematics, University of Maryland, College Park,
MD 20742 USA.

(lcw@math.umd.edu)

ANDREW WILES

Department of Mathematics, Princeton University, Princeton, NJ 08544
USA.

(wiles@math.princeton.edu)

Schedule of Lectures

Wednesday, August 9, 1995

- 9:00–10:00 Glenn Stevens, *Overview of the proof of Fermat's Last Theorem*
10:30–11:30 Joseph Silverman, *Geometry of elliptic curves*
1:30–2:30 Jaap Top, *Modular curves*
3:00–4:00 Larry Washington, *Galois cohomology and Tate duality*

Thursday, August 10, 1995

- 9:00–10:00 Joseph Silverman, *Arithmetic of elliptic curves*
10:30–11:30 Jaap Top, *The Eichler-Shimura relations*
1:30–2:30 John Tate, *Finite group schemes*
3:00–4:00 Jerry Tunnell, *Modularity of $\bar{\rho}_{E,3}$*

Friday, August 11, 1995

- 9:00–10:00 Dick Gross, *Serre's Conjectures*
10:30–11:30 Barry Mazur, *Deformations of Galois representations: Introduction*
1:30–2:30 Hendrik Lenstra, Jr., *Explicit construction of deformation rings*
3:00–4:00 Jerry Tunnell, *On the Langlands Program*

Saturday, August 12, 1995

- 9:00–10:00 Jerry Tunnell, *Proof of certain cases of Artin's Conjecture*
10:30–11:30 Barry Mazur, *Deformations of Galois representations: Examples*
1:30–2:30 Dick Gross, *Ribet's Theorem*
3:00–4:00 Gerhard Frey, *Fermat's Last Theorem and elliptic curves*

Monday, August 14, 1995

- 9:00–10:00 Jacques Tilouine, *Hecke algebras and the Gorenstein property*
- 10:30–11:30 René Schoof, *The Wiles-Lenstra criterion for complete intersections*
- 1:30–2:30 Barry Mazur, *The tangent space and the module of Kähler differentials of the universal deformation ring*
- 3:00–4:00 Ken Ribet, *p -adic modular deformations of mod p modular representations*

Tuesday, August 15, 1995

- 9:00–10:00 René Schoof, *The Wiles-Faltings criterion for complete intersections*
- 10:30–11:30 Brian Conrad, *The flat deformation functor*
- 1:30–2:30 Larry Washington, *Computations of Galois cohomology*
- 3:00–4:00 Gary Cornell, *Sociology, history and the first case of Fermat*

Wednesday, August 16, 1995

- 9:00–10:00 Ken Ribet, *Wiles' "Main Conjecture"*
- 10:30–11:30 Ehud de Shalit, *Modularity of the universal deformation ring (the minimal case)*

Thursday, August 17, 1995

- 9:00–10:00 Alice Silverberg, *Explicit families of elliptic curves with prescribed mod n representations*
- 10:30–11:30 Ehud de Shalit, *Estimating Selmer groups*
- 1:30–2:30 Ken Ribet, *Non-minimal deformations (the "induction step")*
- 3:00–4:00 Michael Rosen, *Remarks on the history of Fermat's Last Theorem: 1844 to 1984*

Friday, August 18, 1995

- 9:00–10:00 Fred Diamond, *An extension of Wiles' results*
- 10:30–11:30 Karl Rubin, *Modularity of mod 5 representations*
- 1:30–2:30 Henri Darmon, *Consequences and applications of Wiles' theorem on modular elliptic curves*
- 3:00–4:00 Andrew Wiles, *Modularity of semistable elliptic curves: Overview of the proof*

Introduction

The chapters of this book are expanded versions of the lectures given at the BU conference. They are intended to introduce the many ideas and techniques used by Wiles in his proof that every (semi-stable) elliptic curve over \mathbf{Q} is modular, and to explain how Wiles' result combined with Ribet's theorem implies the validity of Fermat's Last Theorem.

The first chapter contains an overview of the complete proof, and it is followed by introductory chapters surveying the basic theory of elliptic curves (Chapter II), modular functions and curves (Chapter III), Galois cohomology (Chapter IV), and finite group schemes (Chapter V). Next we turn to the representation theory which lies at the core of Wiles' proof. Chapter VI gives an introduction to automorphic representations and the Langlands-Tunnell theorem, which provides the crucial first step that a certain mod 3 representation is modular. Chapter VII describes Serre's conjectures and the known cases which give the link between modularity of elliptic curves and Fermat's Last Theorem. After this come chapters on deformations of Galois representations (Chapter VIII) and universal deformation rings (Chapter IX), followed by chapters on Hecke algebras (Chapter X) and complete intersections (Chapter XI). Chapters XII and XIV contain the heart of Wiles' proof, with a brief interlude (Chapter XIII) devoted to representability of the flat deformation functor. The final step in Wiles' proof, the so-called "3-5 shift," is discussed in Chapters XV and XVI, and Diamond's relaxation of the semi-stability condition is described in Chapter XVII. The volume concludes by looking both backward and forward in time, with two chapters (Chapters XVIII and XIX) describing some of the "pre-modular" history of Fermat's Last Theorem, and two chapters (Chapters XX and XXI) placing Wiles' theorem into a more general Diophantine context and giving some ideas of possible future applications.

As the preceding brief summary will have made clear, the proof of Wiles' theorem is extremely intricate and draws on tools from many areas of mathematics. The editors hope that this volume will help everyone, student and professional mathematician alike, who wants to study the details of what is surely one of the most memorable mathematical achievements of this century.

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	
Serre's Conjectures	209
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	
An Introduction to the Deformation Theory of Galois Representations	243
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	
Explicit Construction of Universal Deformation Rings	313
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	
Hecke Algebras and the Gorenstein Property	327
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