Graduate Texts in Mathematics 151

Springer Science+Business Media, LLC

Graduate Texts in Mathematics

1 TAKEUTI/ZARING. Introduction to Axiomatic Set Theory. 2nd ed.
2 OXTOBY. Measure and Category. 2nd ed.
3 SCHAEFER. Topological Vector Spaces. 2nd ed.
4 HILTON/STAMMBACH. A Course in Homological Algebra. 2nd ed.
5 MAC LANE. Categories for the Working Mathematician. 2nd ed.
6 HUGHES/PIPER. Projective Planes.
7 SERRE. A Course in Arithmetic.
8 TAKEUTI/ZARING. Axiomatic Set Theory.
9 HUMPHREYS. Introduction to Lie Algebras and Representation Theory.
10 COHEN. A Course in Simple Homotopy Theory.
11 CONWAY. Functions of One Complex Variable I. 2nd ed.
12 BEALS. Advanced Mathematical Analysis.
13 ANDERSON/FULLER. Rings and Categories of Modules. 2nd ed.
14 GOLUBITSKY/GUILLEMIN. Stable Mappings and Their Singularities.
15 BERBERIAN. Lectures in Functional Analysis and Operator Theory.
16 WINTER. The Structure of Fields.
17 ROSENBLATT. Random Processes. 2nd ed.
18 HALMOS. Measure Theory.
19 HALMOS. A Hilbert Space Problem Book. 2nd ed.
20 HUSEMOLLER. Fibre Bundles. 3rd ed.
21 HUMPHREYS. Linear Algebraic Groups.
22 BARNES/MACK. An Algebraic Introduction to Mathematical Logic.
23 GREUB. Linear Algebra. 4th ed.
24 HOLMES. Geometric Functional Analysis and Its Applications.
25 HEWITT/STROMBERG. Real and Abstract Analysis.
26 MANES. Algebraic Theories.
27 KELLEY. General Topology.
28 ZARISKI/SAMUEL. Commutative Algebra. Vol.I.
29 ZARISKI/SAMUEL. Commutative Algebra. Vol.II.
30 JACOBSON. Lectures in Abstract Algebra I. Basic Concepts.
31 JACOBSON. Lectures in Abstract Algebra II. Linear Algebra.
32 JACOBSON. Lectures in Abstract Algebra III. Theory of Fields and Galois Theory.
33 HIRSCH. Differential Topology.
34 SPITZER. Principles of Random Walk. 2nd ed.
35 ALEXANDER/WERMER. Several Complex Variables and Banach Algebras. 3rd ed.
36 KELLEY/NAMIOKA et al. Linear Topological Spaces.
37 MONK. Mathematical Logic.
38 GRAUERT/FRITZSCHE. Several Complex Variables.
39 ARVESON. An Invitation to C^*-Algebras.
40 KEMENY/SNELL/KNAPP. Denumerable Markov Chains. 2nd ed.
41 APOSTOL. Modular Functions and Dirichlet Series in Number Theory. 2nd ed.
42 SERRE. Linear Representations of Finite Groups.
43 GILLMAN/JERISON. Rings of Continuous Functions.
44 KENDIG. Elementary Algebraic Geometry.
45 LOÈVE. Probability Theory I. 4th ed.
46 LOÈVE. Probability Theory II. 4th ed.
47 MOISE. Geometric Topology in Dimensions 2 and 3.
48 SACHS/WU. General Relativity for Mathematicians.
49 GRUENBERG/WEIR. Linear Geometry. 2nd ed.
50 EDWARDS. Fermat's Last Theorem.
51 KLINGENBERG. A Course in Differential Geometry.
52 HARTSHORNE. Algebraic Geometry.
53 MANIN. A Course in Mathematical Logic.
54 GRAVER/WATKINS. Combinatorics with Emphasis on the Theory of Graphs.
55 BROWN/PEARCY. Introduction to Operator Theory I: Elements of Functional Analysis.
56 MASSEY. Algebraic Topology: An Introduction.
57 CROWELL/FOX. Introduction to Knot Theory.
58 KOBLITZ. p-adic Numbers, p-adic Analysis, and Zeta-Functions. 2nd ed.
59 LANG. Cyclotomic Fields.
60 ARNOLD. Mathematical Methods in Classical Mechanics. 2nd ed.
61 WHITEHEAD. Elements of Homotopy Theory.

(continued after index)

Joseph H. Silverman

Advanced Topics in the Arithmetic of Elliptic Curves

With 17 Illustrations

Springer

Joseph H. Silverman
Mathematics Department
Brown University
Providence, RI 02912
USA
jhs@math.brown.edu

Mathematics Subject Classifications (1991): 14-01, 11Gxx, 14Gxx, 14H52

Library of Congress Cataloging-in-Publication Data
Silverman, Joseph H., 1955-
Advanced topics in the arithmetic of elliptic curves / Joseph H. Silverman.
p. cm. – (Graduate texts in mathematics ; v. 151)
Includes bibliographical references and index.
ISBN 978-0-387-94328-2 ISBN 978-1-4612-0851-8 (eBook)
DOI 10.1007/978-1-4612-0851-8
1. Curves, Elliptic. 2. Curves, Algebraic. 3. Arithmetic.
I. Title. II. Series.
QA567.S442 1994
516.3'52–dc20 94-21787

Printed on acid-free paper.

Production managed by Hal Henglein; manufacturing supervised by Vincent Scelta.
Photocomposed copy prepared from the author's TeX file.

9 8 7 6 5 4 3 2 (Corrected second printing, 1999)

ISBN 978-0-387-94328-2 SPIN 10727882

For Susan

Preface

In the introduction to the first volume of *The Arithmetic of Elliptic Curves* (Springer-Verlag, 1986), I observed that "the theory of elliptic curves is rich, varied, and amazingly vast," and as a consequence, "many important topics had to be omitted." I included a brief introduction to ten additional topics as an appendix to the first volume, with the tacit understanding that eventually there might be a second volume containing the details. You are now holding that second volume.

Unfortunately, it turned out that even those ten topics would not fit into a single book, so I was forced to make some choices. The following material is covered in this book:

I. Elliptic and modular functions for the full modular group.
II. Elliptic curves with complex multiplication.
III. Elliptic surfaces and specialization theorems.
IV. Néron models, Kodaira-Néron classification of special fibers, Tate's algorithm, and Ogg's conductor-discriminant formula.
V. Tate's theory of q-curves over p-adic fields.
VI. Néron's theory of canonical local height functions.

So what's still missing? First and foremost is the theory of modular curves of higher level and the associated modular parametrizations of elliptic curves. There is little question that this is currently the hottest topic in the theory of elliptic curves, but any adequate treatment would seem to require (at least) an entire book of its own. (For a nice introduction, see Knapp [1].) Other topics that I have left out in order to keep this book at a manageable size include the description of the image of the ℓ-adic representation attached to an elliptic curve and local and global duality theory. Thus, at best, this book covers approximately half of the material described in the appendix to the first volume. I apologize to those who may feel disappointed, either at the incompleteness or at the choice of particular topics.

In addition to the complete areas which have been omitted, there are several topics which might have been naturally included if space had been available. These include a description of Iwasawa theory in Chapter II,

the analytic theory of p-adic functions (rigid analysis) in Chapter V, and Arakelov intersection theory in Chapter VI.

It has now been almost a decade since the first volume was written. During that decade the already vast mathematical literature on elliptic curves has continued to explode, with exciting new results appearing with astonishing rapidity. Despite the many omissions detailed above, I am hopeful that this book will prove useful, both for those who want to learn about elliptic curves and for those who hope to advance the frontiers of our knowledge. I offer all of you the best of luck in your explorations!

Computer Packages

There are several computer packages now available for performing computations on elliptic curves. PARI and SIMATH have many built-in elliptic curve functions, there are packages available for commercial programs such as Mathematica and Maple, and the author has written a small stand-alone program which runs on Macintosh computers. Listed below are addresses, current as of March 1994, where these packages may be acquired via anonymous ftp.

PARI (includes many elliptic curve functions)
- math.ucla.edu 128.97.4.254
- megrez.ceremab.u-bordeaux.fr 147.210.16.17
  - (directory pub/pari)
  - (unix, mac, msdos, amiga versions available)

SIMATH (includes many elliptic curve functions)
- ftp.math.orst.edu
- ftp.math.uni-sb.de

apecs (arithmetic of plane elliptic curves, Maple package)
- math.mcgill.ca 132.206.1.20
  - (directory pub/apecs)

Elliptic Curve Calculator (Mathematica package)

Elliptic Curve Calculator (stand-alone Macintosh program)
- gauss.math.brown.edu 128.148.194.40
  - (directory dist/EllipticCurve)

A description of many of the algorithms used for doing computations on elliptic curves can be found in H. Cohen [1, Ch. 7] and Cremona [1].

Acknowledgments

I would like to thank Peter Landweber and David Rohrlich for their careful reading of much of the original draft of this book. My thanks also go to the many people who offered corrections, suggestions, and encouragement, including Michael Artin, Ian Connell, Rob Gross, Marc Hindry, Paul Lockhart, Jonathan Lubin, Masato Kuwata, Elisabetta Manduchi, Michael Rosen, Glenn Stevens, Felipé Voloch, and Siman Wong.

As in the first volume, I have consulted a great many sources while writing this book. Citations have been included for major theorems, but

many results which are now considered "standard" have been presented as such. In any case, I claim no originality for any of the unlabeled theorems in this book, and apologize in advance to anyone who may feel slighted. Sources which I found especially useful included the following:

Chapter I	Apostol [1], Lang [1,2,3], Serre [3], Shimura [1]
Chapter II	Lang [1], Serre [6], Shimura [1]
Chapter IV	Artin [1], Bosch-Lütkebohmert-Raynaud [1], Tate [2]
Chapter V	Robert [1], Tate [9]
Chapter VI	Lang [3,4], Tate [3]

I would like to thank John Tate for providing me with a copy of his unpublished manuscript (Tate [9]) containing the theory of q-curves over complete fields. This material, some of which is taken verbatim from Professor Tate's manuscript, forms the bulk of Chapter V, Section 3. In addition, the description of Tate's algorithm in Chapter IV, Section 9, follows very closely Tate's original exposition in [2], and I appreciate his allowing me to include this material.

Portions of this book were written while I was visiting the University of Paris VII (1992), IHES (1992), Boston University (1993), and Harvard (1994). I would like to thank everyone at these institutions for their hospitality during my stay.

Finally, and most importantly, I would like to thank my wife Susan for her constant love and understanding, and Debby, Danny, and Jonathan for providing all of those wonderful distractions so necessary for a truly happy life.

Joseph H. Silverman
March 27, 1994

Acknowledgments for the Second Printing

I would like to thank the following people who kindly provided corrections which have been incorporated in this second revised printing: Andrew Baker, Brian Conrad, Guy Diaz, Darrin Doud, Lisa Fastenberg, Benji Fisher, Boris Iskra, Steve Harding, Sharon Kineke, Joan-C. Lario, Yihsiang Liow, Ken Ono, Michael Reid, Ottavio Rizzo, David Rohrlich, Samir Siksek, Tonghai Yang, Horst Zimmer.

Providence, Rhode Island *February, 1999*

Contents