Graduate Texts in Mathematics 106

Graduate Texts in Mathematics

1 TAKEUTI/ZARING. Introduction to Axiomatic Set Theory. 2nd ed.
2 OXTOBY. Measure and Category. 2nd ed.
3 SCHAEFFER. Topological Vector Spaces.
4 HILTON/STAMMBACH. A Course in Homological Algebra.
5 MACLANE. Categories for the Working Mathematician.
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. 2nd ed.
12 BEALS. Advanced Mathematical Analysis.
13 ANDERSON/FULLER. Rings and Categories of Modules.
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., revised.
20 HUSEMOLLER. Fibre Bundles. 2nd 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 WERMER. Banach Algebras and Several Complex Variables. 2nd 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.
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.

continued after Index

Joseph H. Silverman

The Arithmetic of Elliptic Curves

With 13 Illustrations

Springer Science+Business Media, LLC

Joseph H. Silverman
Department of Mathematics
Massachusetts Institute of Technology
Cambridge, MA 02139
U.S.A.

AMS Subject Classifications: 14-01, 14G99, 14H05, 14H251, 14K15

Library of Congress Cataloging-in-Publication Data
Silverman, Joseph H.
The arithmetic of elliptic curves.
(Graduate texts in mathematics ; 106)
Bibliography: p.
Includes index.
1. Curves, Elliptic. 2. Curves, Algebraic.
3. Arithmetic—1961– . I. Title. II. Series.
QA567.S44 1985 516.3′5 85-17182

Originally published by Springer-Verlag New York Inc. in 1986
Softcover reprint of the hardcover 1st edition 1986

Typeset by Asco Trade Typesetting Ltd., Hong Kong.

9 8 7 6 5 4 3 2 1

ISBN 978-1-4757-1922-2 ISBN 978-1-4757-1920-8 (eBook)
DOI 10.1007/978-1-4757-1920-8

Preface

The preface to a textbook frequently contains the author's justification for offering the public "another book" on the given subject. For our chosen topic, the arithmetic of elliptic curves, there is little need for such an apologia. Considering the vast amount of research currently being done in this area, the paucity of introductory texts is somewhat surprising. Parts of the theory are contained in various books of Lang (especially [La 3] and [La 5]); and there are books of Koblitz ([Kob]) and Robert ([Rob], now out of print) which concentrate mostly on the analytic and modular theory. In addition, survey articles have been written by Cassels ([Ca 7], really a short book) and Tate ([Ta 5], which is beautifully written, but includes no proofs). Thus the author hopes that this volume will fill a real need, both for the serious student who wishes to learn the basic facts about the arithmetic of elliptic curves; and for the research mathematician who needs a reference source for those same basic facts.

Our approach is more algebraic than that taken in, say, [La 3] or [La 5], where many of the basic theorems are derived using complex analytic methods and the Lefschetz principle. For this reason, we have had to rely somewhat more on techniques from algebraic geometry. However, the geometry of (smooth) curves, which is essentially all that we use, does not require a great deal of machinery. And the small price paid in learning a little bit of algebraic geometry is amply repaid in a unity of exposition which (to the author) seems to be lacking when one makes extensive use of either the Lefschetz principle or lengthy (but elementary) calculations with explicit polynomial equations.

This last point is worth amplifying. It has been the author's experience that "elementary" proofs requiring page after page of algebra tend to be quite uninstructive. A student may be able to verify such a proof, line by line, and at the end will agree that the proof is complete. But little true understanding results from such a procedure. In this book, our policy is always to state when a result can be proven by such an elementary calculation, indicate briefly how that calculation might be done, and then give a more enlightening proof which is based on general principles.

The basic (global) theorems in the arithmetic of elliptic curves are the Mordell–Weil theorem, which is proven in chapter VIII and analyzed more closely in chapter X; and Siegel's theorem, which is proven in chapter IX. The reader desiring to reach these results fairly rapidly might take the following path:

I and II (briefly review), III (§1–8), IV (§1–6), V (§1),
VII (§1–5), VIII (§1–6), IX (§1–7), X (§1–6).

This material also makes a good one-semester course, possibly with some time left at the end for special topics. The present volume is built around the notes for such a course, taught by the author at M.I.T. during the spring term of 1983. [Of course, there are many other possibilities. For example, one might include all of chapters V and VI, skipping IX and (if pressed for time) X.] Other important topics in the arithmetic of elliptic curves, which do not appear in this volume due to time and space limitations, are briefly discussed in appendix C.

It is certainly true that some of the deepest results in this subject, such as Mazur's theorem bounding torsion over $\mathbb{Q}$ and Faltings' proof of the isogeny conjecture, require many of the resources of modern "SGA-style" algebraic geometry. On the other hand, one needs no machinery at all to write down the equation of an elliptic curve and to do explicit computations with it; and so there are many important theorems whose proof requires nothing more than cleverness and hard work. Whether your inclination leans toward heavy machinery or imaginative calculations, you will find much that remains to be discovered in the arithmetic theory of elliptic curves. Happy hunting!

Acknowledgments

In writing this book, I have consulted a great many sources. Citations have been included for major theorems, but many results which are now considered "standard" have been presented as such. In any case, I can claim no originality for any of the unlabeled theorems in this book, and apologize in advance to anyone who may feel slighted. The excellent survey articles of Cassels [Ca 7] and Tate [Ta 5] served as guidelines for organizing the material. (The reader is especially urged to peruse the latter.) In addition to [Ca 7] and [Ta 5], other sources which were extensively consulted include [La 5], [La 7], [Mum], [Rob], and [Se 10].

It would not be possible to catalogue all of the mathematicians from whom

I learned this beautiful subject; but to all of them, my deepest thanks. I would especially like to thank John Tate, Barry Mazur, Serge Lang, and the "Elliptic Curves Seminar" group at Harvard (1977–1982), whose help and inspiration set me on the road which led to this book. I would also like to thank David Rohrlich and Bill McCallum for their careful reading of the original draft, Gary Cornell and the editorial staff of Springer-Verlag for encouraging me to undertake this project in the first place, and Ann Clee for her meticulous preparation of the manuscript. Finally, I would like to thank my wife, Susan, for her patience and understanding through the turbulent times during which this book was written; and also Deborah and Daniel, for providing most of the turbulence.

Cambridge, Massachusetts
September, 1985

JOSEPH H. SILVERMAN

Contents