Undergraduate Texts in Mathematics

Editors

S. Axler

F. W. Gehring

K. A. Ribet

Springer Science+Business Media, LLC

Undergraduate Texts in Mathematics

Abbott: Understanding Analysis.
Anglin: Mathematics: A Concise History and Philosophy.
Readings in Mathematics.
Anglin/Lambek: The Heritage of Thales.
Readings in Mathematics.
Apostol: Introduction to Analytic Number Theory. Second edition.
Armstrong: Basic Topology.
Armstrong: Groups and Symmetry.
Axler: Linear Algebra Done Right. Second edition.
Beardon: Limits: A New Approach to Real Analysis.
Bak/Newman: Complex Analysis. Second edition.
Banchoff/Wermer: Linear Algebra Through Geometry. Second edition.
Berberian: A First Course in Real Analysis.
Bix: Conics and Cubics: A Concrete Introduction to Algebraic Curves.
Brémaud: An Introduction to Probabilistic Modeling.
Bressoud: Factorization and Primality Testing.
Bressoud: Second Year Calculus.
Readings in Mathematics.
Brickman: Mathematical Introduction to Linear Programming and Game Theory.
Browder: Mathematical Analysis: An Introduction.
Buchmann: Introduction to Cryptography.
Buskes/van Rooij: Topological Spaces: From Distance to Neighborhood.
Callahan: The Geometry of Spacetime: An Introduction to Special and General Relavitity.
Carter/van Brunt: The Lebesgue–Stieltjes Integral: A Practical Introduction.
Cederberg: A Course in Modern Geometries. Second edition.
Childs: A Concrete Introduction to Higher Algebra. Second edition.
Chung/AitSahlia: Elementary Probability Theory: With Stochastic Processes and an Introduction to Mathematical Finance. Fourth edition.
Cox/Little/O'Shea: Ideals, Varieties, and Algorithms. Second edition.
Croom: Basic Concepts of Algebraic Topology.
Curtis: Linear Algebra: An Introductory Approach. Fourth edition.
Devlin: The Joy of Sets: Fundamentals of Contemporary Set Theory. Second edition.
Dixmier: General Topology.
Driver: Why Math?
Ebbinghaus/Flum/Thomas: Mathematical Logic. Second edition.
Edgar: Measure, Topology, and Fractal Geometry.
Elaydi: An Introduction to Difference Equations. Second edition.
Erdős/Surányi: Topics in the Theory of Numbers.
Estep: Practical Analysis in One Variable.
Exner: An Accompaniment to Higher Mathematics.
Exner: Inside Calculus.
Fine/Rosenberger: The Fundamental Theory of Algebra.
Fischer: Intermediate Real Analysis.
Flanigan/Kazdan: Calculus Two: Linear and Nonlinear Functions. Second edition.
Fleming: Functions of Several Variables. Second edition.
Foulds: Combinatorial Optimization for Undergraduates.
Foulds: Optimization Techniques: An Introduction.
Franklin: Methods of Mathematical Economics.
Frazier: An Introduction to Wavelets Through Linear Algebra.

(continued after index)

Joseph H. Silverman John Tate

Rational Points on Elliptic Curves

With 34 Illustrations

Springer

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

John Tate
Department of Mathematics
University of Texas at Austin
Austin, TX 78712
USA

Mathematics Subject Classification (2000): 11G05, 11D25

Library of Congress Cataloging-in-Publication Data
Silverman, Joseph H., 1955–
Rational points on elliptic curves / Joseph H. Silverman, John Tate.
p. cm. — (Undergraduate texts in mathematics)
Includes bibliographical references and index.
ISBN 978-1-4419-3101-6 ISBN 978-1-4757-4252-7 (eBook)
DOI 10.1007/978-1-4757-4252-7
1. Curves, Elliptic. 2. Diophantine analysis. I. Tate, John Torrence, 1925– II. Title. III. Series.
QA567.2.E44S55 1992
516.3'52—dc20 92-4669

Printed on acid-free paper.

9 8 7 6 SPIN 11011361

springeronline.com

Preface

In 1961 the second author delivered a series of lectures at Haverford College on the subject of "Rational Points on Cubic Curves." These lectures, intended for junior and senior mathematics majors, were recorded, transcribed, and printed in mimeograph form. Since that time they have been widely distributed as photocopies of ever decreasing legibility, and portions have appeared in various textbooks (Husemöller [1], Chahal [1]), but they have never appeared in their entirety. In view of the recent interest in the theory of elliptic curves for subjects ranging from cryptography (Lenstra [1], Koblitz [2]) to physics (Luck-Moussa-Waldschmidt [1]), as well as the tremendous purely mathematical activity in this area, it seems a propitious time to publish an expanded version of those original notes suitable for presentation to an advanced undergraduate audience.

We have attempted to maintain much of the informality of the original Haverford lectures. Our main goal in doing this has been to write a textbook in a technically difficult field which is "readable" by the average undergraduate mathematics major. We hope we have succeeded in this goal. The most obvious drawback to such an approach is that we have not been entirely rigorous in all of our proofs. In particular, much of the foundational material on elliptic curves presented in Chapter I is meant to explain and convince, rather than to rigorously prove. Of course, the necessary algebraic geometry can mostly be developed in one moderately long chapter, as we have done in Appendix A. But the emphasis of this book is on the number theoretic aspects of elliptic curves; and we feel that an informal approach to the underlying geometry is permissible, because it allows us more rapid access to the number theory. For those who wish to delve more deeply into the geometry, there are several good books on the theory of algebraic curves suitable for an undergraduate course, such as Reid [1], Walker [1] and Brieskorn-Knörrer [1]. In the later chapters we have generally provided all of the details for the proofs of the main theorems.

The original Haverford lectures make up Chapters I, II, III, and the first two sections of Chapter IV. In a few places we have added a small amount of explanatory material, references have been updated to include some discoveries made since 1961, and a large number of exercises have

been added. But those who have seen the original mimeographed notes will recognize that the changes have been kept to a minimum. In particular, the emphasis is still on proving (special cases of) the fundamental theorems in the subject: (1) the Nagell-Lutz theorem, which gives a precise procedure for finding all of the rational points of finite order on an elliptic curve; (2) Mordell's theorem, which says that the group of rational points on an elliptic curve is finitely generated; (3) a special case of Hasse's theorem, due to Gauss, which describes the number of points on an elliptic curve defined over a finite field.

In the last section of Chapter IV we have described Lenstra's elliptic curve algorithm for factoring large integers. This is one of the recent applications of elliptic curves to the "real world," to wit the attempt to break certain widely used public key ciphers. We have restricted ourselves to describing the factorization algorithm itself, since there have been many popular descriptions of the corresponding ciphers. (See, for example, Koblitz [2].)

Chapters V and VI are new. Chapter V deals with integer points on elliptic curves. Section 2 of Chapter V is loosely based on an IAP undergraduate lecture given by the first author at MIT in 1983. The remaining sections of Chapter V contain a proof of a special case of Siegel's theorem, which asserts that an elliptic curve has only finitely many integral points. The proof, based on Thue's method of Diophantine approximation, is elementary, but intricate. However, in view of Vojta's [1] and Faltings' [1] recent spectacular applications of Diophantine approximation techniques, it seems appropriate to introduce this subject at an undergraduate level. Chapter VI gives an introduction to the theory of complex multiplication. Elliptic curves with complex multiplication arise in many different contexts in number theory and in other areas of mathematics. The goal of Chapter VI is to explain how points of finite order on elliptic curves with complex multiplication can be used to generate extension fields with abelian Galois groups, much as roots of unity generate abelian extensions of the rational numbers. For Chapter VI only, we have assumed that the reader is familiar with the rudiments of field theory and Galois theory.

Finally, we have included an appendix giving an introduction to projective geometry, with an especial emphasis on curves in the projective plane. The first three sections of Appendix A provide the background needed for reading the rest of the book. In Section 4 of Appendix A we give an elementary proof of Bezout's theorem, and in Section 5 we provide a rigorous discussion of the reduction modulo p map and explain why it induces a homomorphism on the rational points of an elliptic curve.

The contents of this book should form a leisurely semester course, with some time left over for additional topics in either algebraic geometry or number theory. The first author has also used this material as a supplementary special topic at the end of an undergraduate course in modern algebra, covering Chapters I, II, and IV (excluding IV §3) in about four weeks of classes. We note that the last five chapters are essentially

independent of one another (except IV §3 depends on the Nagell-Lutz theorem, proven in Chapter II). This gives the instructor maximum freedom in choosing topics if time is short. It also allows students to read portions of the book on their own (e.g., as a suitable project for a reading course or an honors thesis.) We have included many exercises, ranging from easy calculations to published theorems. An exercise marked with a (*) is likely to be somewhat challenging. An exercise marked with (**) is either extremely difficult to solve with the material we cover or actually a currently unsolved problem.

It has been said that "it is possible to write endlessly on elliptic curves."† We heartily agree with this sentiment, but have attempted to resist succumbing to its blandishments. This is especially evident in our frequent decision to prove special cases of general theorems, even when only a few more pages would be required to prove a more general result. Our goal throughout has been to illuminate the coherence and the beauty of the arithmetic theory of elliptic curves; we happily leave the task of being encyclopedic to the authors of more advanced monographs.

Computer Packages

The first author has written two computer packages to perform basic computations on elliptic curves. The first is a stand-alone application which runs on any variety of Macintosh. The second is a collection of *Mathematica* routines with extensive documentation included in the form of Notebooks in Macintosh *Mathematica* format. Instructors are welcome to freely copy and distribute both of these programs. They may be obtained via anonymous ftp at

gauss.math.brown.edu (128.148.194.40)

in the directory dist/EllipticCurve.

Acknowledgments

The authors would like to thank Rob Gross, Emma Previato, Michael Rosen, Seth Padowitz, Chris Towse, Paul van Mulbregt, Eileen O'Sullivan, and the students of Math 153 (especially Jeff Achter and Jeff Humphrey) for reading and providing corrections to the original draft. They would also like to thank Davide Cervone for producing beautiful illustrations from their original jagged diagrams.

† From the introduction to *Elliptic Curves: Diophantine Analysis*, Serge Lang, Springer-Verlag, New York, 1978. Professor Lang follows his assertion with the statement that "This is not a threat," indicating that he, too, has avoided the temptation to write a book of indefinite length.

The first author owes a tremendous debt of gratitude to Susan for her patience and understanding, to Debby for her fluorescent attire brightening up the days, to Danny for his unfailing good humor, and to Jonathan for taking timely naps during critical stages in the preparation of this manuscript.

The second author would like to thank Louis Solomon for the invitation to deliver the Philips Lectures at Haverford College in the Spring of 1961.

Joseph H. Silverman
John Tate

March 27, 1992

Acknowledgments for the Second Printing

The authors would like to thank the following people for sending us suggestions and corrections, many of which have been incorporated into this second printing: G. Allison, D. Appleby, K. Bender, G. Bender, P. Berman, J. Blumenstein, D. Freeman, L. Goldberg, A. Guth, A. Granville, J. Kraft, M. Mossinghoff, R. Pries, K. Ribet, H. Rose, J.-P. Serre, M. Szydlo, J. Tobey, C.R. Videla, J. Wendel.

Joseph H. Silverman
John Tate

June 13, 1994

Contents