Graduate Texts in Mathematics

Dale Husemöller

Elliptic Curves

Second Edition

椭圆曲线 第2版

Springer

世界图书出版公司
www.wpcbj.com.cn

Dale Husemöller

Elliptic Curves

Second Edition

With Appendices by Otto Forster, Ruth Lawrence, and Stefan Theisen

With 42 Illustrations

Springer

图书在版编目（CIP）数据

椭圆曲线：第2版 = Elliptic Curves 2nd：
英文/（德）胡斯迈勒著. —影印本.
—北京：世界图书出版公司北京公司，2011.3
ISBN 978-7-5100-3303-2

Ⅰ.①椭… Ⅱ.①胡… Ⅲ.①椭圆曲线—研究生--教材—英文 Ⅳ.①O187.1

中国版本图书馆CIP数据核字（2011）第029456号

书　　名：	Elliptic Curves 2nd ed.
作　　者：	Dale Husemöller
中 译 名：	椭圆曲线 第2版
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：	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：	21.5
版　　次：	2011年04月
版权登记：	图字：01-2011-0424
书　　号：	978-7-5100-3303-2/O·880　　**定　　价：** 65.00元

Dale Husemöller
Max-Planck-Institut für Mathematik
Vivatsgasse 7
D-53111 Bonn
Germany
dale@mpim-bonn.mpg.de

Mathematics Subject Classification (2000): 14-01, 14H52

Library of Congress Cataloging-in-Publication Data
Husemöller, Dale.
Elliptic curves.— 2nd ed. / Dale Husemöller ; with appendices by Stefan Theisen, Otto Forster, and Ruth Lawrence.
p. cm. — (Graduate texts in mathematics; 111)
Includes bibliographical references and index.
ISBN 0-387-95490-2 (alk. paper)
1. Curves, Elliptic. 2. Curves, Algebraic. 3. Group schemes (Mathematics) I. Title. II. Series.
QA567 .H897 2002
516.3'52—dc21 2002067016

ISBN 0-387-95490-2

springeronline.com

To
Robert
and the memory of
Roger,
with whom I first learned
the meaning of collaboration

Preface to the Second Edition

The second edition builds on the first in several ways. There are three new chapters which survey recent directions and extensions of the theory, and there are two new appendices. Then there are numerous additions to the original text. For example, a very elementary addition is another parametrization which the author learned from Don Zagier $y^2 = x^3 - 3\alpha x + 2\beta$ of the basic cubic equation. This parametrization is useful for a detailed description of elliptic curves over the real numbers.

The three new chapters are Chapters 18, 19, and 20. Chapter 18, on Fermat's Last Theorem, is designed to point out which material in the earlier chapters is relevant as background for reading Wiles' paper on the subject together with further developments by Taylor and Diamond. The statement which we call the modular curve conjecture has a long history associated with Shimura, Taniyama, and Weil over the last fifty years. Its relation to Fermat, starting with the clever observation of Frey ending in the complete proof by Ribet with many contributions of Serre, was already mentioned in the first edition. The proof for a broad class of curves by Wiles was sufficient to establish Fermat's last theorem. Chapter 18 is an introduction to the papers on the modular curve conjecture and some indication of the proof.

Chapter 19 is an introduction to K3 surfaces and the higher dimensional Calabi–Yau manifolds. One of the motivations for producing the second edition was the utility of the first edition for people considering examples of fibrings of three dimensional Calabi–Yau varieties. Abelian varieties form one class of generalizations of elliptic curves to higher dimensions, and K3 surfaces and general Calabi–Yau manifolds constitute a second class.

Chapter 20 is an extension of earlier material on families of elliptic curves where the family itself is considered as a higher dimensional variety fibered by elliptic curves. The first two cases are one dimensional parameter spaces where the family is two dimensional, hence a surface two dimensional surface parameter spaces where the family is three dimensional. There is the question of, given a surface or a three dimensional variety, does it admit a fibration by elliptic curves with a finite number of exceptional singular fibres. This question can be taken as the point of departure for the Enriques classification of surfaces.

There are three new appendices, one by Stefan Theisen on the role of Calabi–Yau manifolds in string theory and one by Otto Forster on the use of elliptic curves in computing theory and coding theory. In the third appendix we discuss the role of elliptic curves in homotopy theory. In these three introductions the reader can get a clue to the far-reaching implications of the theory of elliptic curves in mathematical sciences.

During the final production of this edition, the ICM 2002 manuscript of Mike Hopkins became available. This report outlines the role of elliptic curves in homotopy theory. Elliptic curves appear in the form of the Weierstasse equation and its related changes of variable. The equations and the changes of variable are coded in an algebraic structure called a Hopf algebroid, and this Hopf algebroid is related to a cohomology theory called topological modular forms. Hopkins and his coworkers have used this theory in several directions, one being the explanation of elements in stable homotopy up to degree 60. In the third appendix we explain how what we described in Chapter 3 leads to the Weierstrass Hopf algebroid making a link with Hopkins' paper.

Max-Planck-Institut für Mathematik
Bonn, Germany

Dale Husemöller

Preface to the First Edition

The book divides naturally into several parts according to the level of the material, the background required of the reader, and the style of presentation with respect to details of proofs. For example, the first part, to Chapter 6, is undergraduate in level, the second part requires a background in Galois theory and the third some complex analysis, while the last parts, from Chapter 12 on, are mostly at graduate level. A general outline of much of the material can be found in Tate's colloquium lectures reproduced as an article in *Inventiones* [1974].

The first part grew out of Tate's 1961 Haverford Philips Lectures as an attempt to write something for publication closely related to the original Tate notes which were more or less taken from the tape recording of the lectures themselves. This includes parts of the Introduction and the first six chapters. The aim of this part is to prove, by elementary methods, the Mordell theorem on the finite generation of the rational points on elliptic curves defined over the rational numbers.

In 1970 Tate returned to Haverford to give again, in revised form, the original lectures of 1961 and to extend the material so that it would be suitable for publication. This led to a broader plan for the book.

The second part, consisting of Chapters 7 and 8, recasts the arguments used in the proof of the Mordell theorem into the context of Galois cohomology and descent theory. The background material in Galois theory that is required is surveyed at the beginnng of Chapter 7 for the convenience of the reader.

The third part, consisting of Chapters 9, 10, and 11, is on analytic theory. A background in complex analysis is assumed and in Chapter 10 elementary results on p-adic fields, some of which were introduced in Chapter 5, are used in our discussion of Tate's theory of p-adic theta functions. This section is based on Tate's 1972 Haverford Philips Lectures.

Max-Planck-Institut für Mathematik
Bonn, Germany

Dale Husemöller

Acknowledgments to the Second Edition

Stefan Theisen, during a period of his work on Calabi–Yau manifolds in conjunction with string theory, brought up many questions in the summer of 1998 which lead to a renewed interest in the subject of elliptic curves on my part.

Otto Forster gave a course in Munich during 2000–2001 on or related to elliptic curves. We had discussions on the subject leading to improvements in the second edition, and at the same time he introduced me to the role of elliptic curves in cryptography.

A reader provided by the publisher made systematic and very useful remarks on everything including mathematical content, exposition, and English throughout the manuscript.

Richard Taylor read a first version of Chapter 18, and his comments were of great use. F. Oort and Don Zagier offered many useful suggestions for improvement of parts of the first edition. In particular the theory of elliptic curves over the real numbers was explained to me by Don.

With the third appendix T. Bauer, M. Joachim, and S. Schwede offered many useful suggestions.

During this period of work on the second edition, I was a research professor from Haverford College, a visitor at the Max Planck Institute for Mathematics in Bonn, a member of the Graduate College and mathematics department in Munich, and a member of the Graduate College in Münster. All of these connections played a significant role in bringing this project to a conclusion.

Max-Planck-Institut für Mathematik
Bonn, Germany

Dale Husemöller

Acknowledgments to the First Edition

Being an amateur in the field of elliptic curves, I would have never completed a project like this without the professional and moral support of a great number of persons and institutions over the long period during which this book was being written.

John Tate's treatment of an advanced subject, the arithmetic of elliptic curves, in an undergraduate context has been an inspiration for me during the last 25 years while at Haverford. The general outline of the project, together with many of the details of the exposition, owe so much to Tate's generous help.

The E.N.S. course by J.-P. Serre of four lectures in June 1970 together with two Haverford lectures on elliptic curves were very important in the early development of the manuscript. I wish to thank him also for many stimulating discussions. Elliptic curves were in the air during the summer seasons at the I.H.E.S. around the early 1970s. I wish to thank P. Deligne, N. Katz, S. Lichtenbaum, and B. Mazur for many helpful conversations during that period. It was the Haverford College Faculty Research Fund that supported many times my stays at the I.H.E.S.

During the year 1974–5, the summer of 1976, the year 1981–2, and the spring of 1986, I was a guest of the Bonn Mathematics Department SFB and later the Max Planck Institute. I wish to thank Professor F. Hirzebruch for making possible time to work in a stimulating atmosphere and for his encouragement in this work. An early version of the first half of the book was the result of a Bonn lecture series on Elliptische Kurven. During these periods, I profited frequently from discussions with G. Harder and A. Ogg.

Conversations with B. Gross were especially important for realizing the final form of the manuscript during the early 1980s. I am very thankful for his encouragement and help. In the spring of 1983 some of the early chapters of the book were used by K. Rubin in the Princeton Junior Seminar, and I thank him for several useful suggestions. During the same time, J. Coates invited me to an Oberwolfach conference on elliptic curves where the final form of the manuscript evolved.

During the final stages of the manuscript, both R. Greenberg and R. Rosen read through the later chapters, and I am grateful for their comments. I would like to thank P. Landweber for a very careful reading of the manuscript and many useful comments.

Ruth Lawrence read the early chapters along with working the exercises. Her contribution was very great with her appendix on the exercises and suggested improvements in the text. I wish to thank her for this very special addition to the book.

Free time from teaching at Haverford College during the year 1985–1986 was made possible by a grant from the Vaughn Foundation. I wish to express my gratitude to Mr. James Vaughn for this support, for this project as well as others, during this difficult last period of the preparation of the manuscript.

Max-Planck-Institut für Mathematik
Bonn, Germany

Dale Husemöller

Contents