

Dale Husemöller

# Elliptic Curves

Second Edition

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

With 42 Illustrations

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

*Editorial Board:*

S. Axler  
Mathematics Department  
San Francisco State  
University  
San Francisco, CA 94132  
USA  
axler@sfsu.edu

F.W. Gehring  
Mathematics Department  
East Hall  
University of Michigan  
Ann Arbor, MI 48109  
USA  
fgehring@math.lsa.umich.edu

K.A. Ribet  
Mathematics Department  
University of California,  
Berkeley  
Berkeley, CA 94720-3840  
USA  
ribet@math.berkeley.edu

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

Printed on acid-free paper.

© 2004, 1987 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 in this publication of trade names, trademarks, services marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

Printed in the United States of America. (TXQ/EB)

9 8 7 6 5 4 3 2 1

SPIN 10877271

Springer-Verlag is a part of *Springer Science+Business Media*

*springeronline.com*

3	Elements of Intersection Theory for Plane Curves .....	50
4	Multiple or Singular Points .....	52
	<b>Appendix to Chapter 2: Factorial Rings and Elimination Theory</b> ....	57
1	Divisibility Properties of Factorial Rings .....	57
2	Factorial Properties of Polynomial Rings .....	59
3	Remarks on Valuations and Algebraic Curves .....	60
4	Resultant of Two Polynomials .....	61
<b>3</b>	<b>Elliptic Curves and Their Isomorphisms</b> .....	65
1	The Group Law on a Nonsingular Cubic .....	65
2	Normal Forms for Cubic Curves .....	67
3	The Discriminant and the Invariant $j$ .....	70
4	Isomorphism Classification in Characteristics $\neq 2, 3$ .....	73
5	Isomorphism Classification in Characteristic 3 .....	75
6	Isomorphism Classification in Characteristic 2 .....	76
7	Singular Cubic Curves .....	80
8	Parameterization of Curves in Characteristic Unequal to 2 or 3 .....	82
<b>4</b>	<b>Families of Elliptic Curves and Geometric Properties of Torsion Points</b> .....	85
1	The Legendre Family .....	85
2	Families of Curves with Points of Order 3: The Hessian Family ....	88
3	The Jacobi Family .....	91
4	Tate's Normal Form for a Cubic with a Torsion Point .....	92
5	An Explicit 2-Isogeny .....	95
6	Examples of Noncyclic Subgroups of Torsion Points .....	101
<b>5</b>	<b>Reduction mod <math>p</math> and Torsion Points</b> .....	103
1	Reduction mod $p$ of Projective Space and Curves .....	103
2	Minimal Normal Forms for an Elliptic Curve .....	106
3	Good Reduction of Elliptic Curves .....	109
4	The Kernel of Reduction mod $p$ and the $p$ -Adic Filtration .....	111
5	Torsion in Elliptic Curves over $\mathbb{Q}$ : Nagell–Lutz Theorem .....	115
6	Computability of Torsion Points on Elliptic Curves from Integrality and Divisibility Properties of Coordinates .....	118
7	Bad Reduction and Potentially Good Reduction .....	120
8	Tate's Theorem on Good Reduction over the Rational Numbers ....	122
<b>6</b>	<b>Proof of Mordell's Finite Generation Theorem</b> .....	125
1	A Condition for Finite Generation of an Abelian Group .....	125
2	Fermat Descent and $x^4 + y^4 = 1$ .....	127
3	Finiteness of $(E(\mathbb{Q}) : 2E(\mathbb{Q}))$ for $E = E[a, b]$ .....	128
4	Finiteness of the Index $(E(k) : 2E(k))$ .....	129
5	Quasilinear and Quasiquadratic Maps .....	132
6	The General Notion of Height on Projective Space .....	135

7	The Canonical Height and Norm on an Elliptic Curve	137
8	The Canonical Height on Projective Spaces over Global Fields	140
<b>7</b>	<b>Galois Cohomology and Isomorphism Classification of Elliptic Curves over Arbitrary Fields</b>	<b>143</b>
1	Galois Theory: Theorems of Dedekind and Artin	143
2	Group Actions on Sets and Groups	146
3	Principal Homogeneous $G$ -Sets and the First Cohomology Set $H^1(G, A)$	148
4	Long Exact Sequence in $G$ -Cohomology	151
5	Some Calculations with Galois Cohomology	153
6	Galois Cohomology Classification of Curves with Given $j$ -Invariant	155
<b>8</b>	<b>Descent and Galois Cohomology</b>	<b>157</b>
1	Homogeneous Spaces over Elliptic Curves	157
2	Primitive Descent Formalism	160
3	Basic Descent Formalism	163
<b>9</b>	<b>Elliptic and Hypergeometric Functions</b>	<b>167</b>
1	Quotients of the Complex Plane by Discrete Subgroups	167
2	Generalities on Elliptic Functions	169
3	The Weierstrass $\wp$ -Function	171
4	The Differential Equation for $\wp(z)$	174
5	Preliminaries on Hypergeometric Functions	179
6	Periods Associated with Elliptic Curves: Elliptic Integrals	183
<b>10</b>	<b>Theta Functions</b>	<b>189</b>
1	Jacobi $q$ -Parametrization: Application to Real Curves	189
2	Introduction to Theta Functions	193
3	Embeddings of a Torus by Theta Functions	195
4	Relation Between Theta Functions and Elliptic Functions	197
5	The Tate Curve	198
6	Introduction to Tate's Theory of $p$ -Adic Theta Functions	203
<b>11</b>	<b>Modular Functions</b>	<b>209</b>
1	Isomorphism and Isogeny Classification of Complex Tori	209
2	Families of Elliptic Curves with Additional Structures	211
3	The Modular Curves $X(N)$ , $X_1(N)$ , and $X_0(N)$	215
4	Modular Functions	220
5	The $L$ -Function of a Modular Form	222
6	Elementary Properties of Euler Products	224
7	Modular Forms for $\Gamma_0(N)$ , $\Gamma_1(N)$ , and $\Gamma(N)$	227
8	Hecke Operators: New Forms	229
9	Modular Polynomials and the Modular Equation	230

<b>12</b>	<b>Endomorphisms of Elliptic Curves</b> . . . . .	233
1	Isogenies and Division Points for Complex Tori . . . . .	233
2	Symplectic Pairings on Lattices and Division Points . . . . .	235
3	Isogenies in the General Case . . . . .	237
4	Endomorphisms and Complex Multiplication . . . . .	241
5	The Tate Module of an Elliptic Curve . . . . .	245
6	Endomorphisms and the Tate Module . . . . .	246
7	Expansions Near the Origin and the Formal Group . . . . .	248
<b>13</b>	<b>Elliptic Curves over Finite Fields</b> . . . . .	253
1	The Riemann Hypothesis for Elliptic Curves over a Finite Field . . . . .	253
2	Generalities on Zeta Functions of Curves over a Finite Field . . . . .	256
3	Definition of Supersingular Elliptic Curves . . . . .	259
4	Number of Supersingular Elliptic Curves . . . . .	263
5	Points of Order $p$ and Supersingular Curves . . . . .	265
6	The Endomorphism Algebra and Supersingular Curves . . . . .	266
7	Summary of Criteria for a Curve To Be Supersingular . . . . .	268
8	Tate's Description of Homomorphisms . . . . .	270
9	Division Polynomial . . . . .	272
<b>14</b>	<b>Elliptic Curves over Local Fields</b> . . . . .	275
1	The Canonical $p$ -Adic Filtration on the Points of an Elliptic Curve over a Local Field . . . . .	275
2	The Néron Minimal Model . . . . .	277
3	Galois Criterion of Good Reduction of Néron–Ogg–Šafarevič . . . . .	280
4	Elliptic Curves over the Real Numbers . . . . .	284
<b>15</b>	<b>Elliptic Curves over Global Fields and <math>\ell</math>-Adic Representations</b> . . . . .	291
1	Minimal Discriminant Normal Cubic Forms over a Dedekind Ring . . . . .	291
2	Generalities on $\ell$ -Adic Representations . . . . .	293
3	Galois Representations and the Néron–Ogg–Šafarevič Criterion in the Global Case . . . . .	296
4	Ramification Properties of $\ell$ -Adic Representations of Number Fields: Čebotarev's Density Theorem . . . . .	298
5	Rationality Properties of Frobenius Elements in $\ell$ -Adic Representations: Variation of $\ell$ . . . . .	301
6	Weight Properties of Frobenius Elements in $\ell$ -Adic Representations: Faltings' Finiteness Theorem . . . . .	303
7	Tate's Conjecture, Šafarevič's Theorem, and Faltings' Proof . . . . .	305
8	Image of $\ell$ -Adic Representations of Elliptic Curves: Serre's Open Image Theorem . . . . .	307

---

# Contents

<b>Preface to the Second Edition</b> .....	vii
<b>Preface to the First Edition</b> .....	ix
<b>Acknowledgments to the Second Edition</b> .....	xi
<b>Acknowledgments to the First Edition</b> .....	xiii
<b>Introduction to Rational Points on Plane Curves</b> .....	1
1 Rational Lines in the Projective Plane .....	2
2 Rational Points on Conics .....	4
3 Pythagoras, Diophantus, and Fermat .....	7
4 Rational Cubics and Mordell's Theorem .....	10
5 The Group Law on Cubic Curves and Elliptic Curves .....	13
6 Rational Points on Rational Curves. Faltings and the Mordell Conjecture .....	17
7 Real and Complex Points on Elliptic Curves .....	19
8 The Elliptic Curve Group Law on the Intersection of Two Quadrics in Projective Three Space .....	20
<b>1 Elementary Properties of the Chord-Tangent Group Law on a Cubic Curve</b> .....	23
1 Chord-Tangent Computational Methods on a Normal Cubic Curve .....	23
2 Illustrations of the Elliptic Curve Group Law .....	28
3 The Curves with Equations $y^2 = x^3 + ax$ and $y^2 = x^3 + a$ .....	34
4 Multiplication by 2 on an Elliptic Curve .....	38
5 Remarks on the Group Law on Singular Cubics .....	41
<b>2 Plane Algebraic Curves</b> .....	45
1 Projective Spaces .....	45
2 Irreducible Plane Algebraic Curves and Hypersurfaces .....	47

<b>16</b>	<b><i>L</i>-Function of an Elliptic Curve and Its Analytic Continuation</b>	309
1	Remarks on Analytic Methods in Arithmetic	309
2	Zeta Functions of Curves over $\mathbb{Q}$	310
3	Hasse–Weil <i>L</i> -Function and the Functional Equation	312
4	Classical Abelian <i>L</i> -Functions and Their Functional Equations	315
5	Größencharacters and Hecke <i>L</i> -Functions	318
6	Deuring’s Theorem on the <i>L</i> -Function of an Elliptic Curve with Complex Multiplication	321
7	Eichler–Shimura Theory	322
8	The Modular Curve Conjecture	324
<b>17</b>	<b>Remarks on the Birch and Swinnerton–Dyer Conjecture</b>	325
1	The Conjecture Relating Rank and Order of Zero	325
2	Rank Conjecture for Curves with Complex Multiplication I, by Coates and Wiles	326
3	Rank Conjecture for Curves with Complex Multiplication II, by Greenberg and Rohrlich	327
4	Rank Conjecture for Modular Curves by Gross and Zagier	328
5	Goldfeld’s Work on the Class Number Problem and Its Relation to the Birch and Swinnerton–Dyer Conjecture	328
6	The Conjecture of Birch and Swinnerton–Dyer on the Leading Term	329
7	Heegner Points and the Derivative of the <i>L</i> -function at $s = 1$ , after Gross and Zagier	330
8	Remarks On Postscript: October 1986	331
<b>18</b>	<b>Remarks on the Modular Elliptic Curves Conjecture and Fermat’s Last Theorem</b>	333
1	Semistable Curves and Tate Modules	334
2	The Frey Curve and the Reduction of Fermat Equation to Modular Elliptic Curves over $\mathbb{Q}$	335
3	Modular Elliptic Curves and the Hecke Algebra	336
4	Hecke Algebras and Tate Modules of Modular Elliptic Curves	338
5	Special Properties of mod 3 Representations	339
6	Deformation Theory and $\ell$ -Adic Representations	339
7	Properties of the Universal Deformation Ring	341
8	Remarks on the Proof of the Opposite Inequality	342
9	Survey of the Nonsemistable Case of the Modular Curve Conjecture	342
<b>19</b>	<b>Higher Dimensional Analogs of Elliptic Curves:</b>	
	<b>Calabi–Yau Varieties</b>	345
1	Smooth Manifolds: Real Differential Geometry	347
2	Complex Analytic Manifolds: Complex Differential Geometry	349
3	Kähler Manifolds	352
4	Connections, Curvature, and Holonomy	356
5	Projective Spaces, Characteristic Classes, and Curvature	361

6	Characterizations of Calabi–Yau Manifolds: First Examples . . . . .	366
7	Examples of Calabi–Yau Varieties from Toric Geometry . . . . .	369
8	Line Bundles and Divisors: Picard and Néron–Severi Groups . . . . .	371
9	Numerical Invariants of Surfaces . . . . .	374
10	Enriques Classification for Surfaces . . . . .	377
11	Introduction to K3 Surfaces . . . . .	378
<b>20</b>	<b>Families of Elliptic Curves . . . . .</b>	<b>383</b>
1	Algebraic and Analytic Geometry . . . . .	384
2	Morphisms Into Projective Spaces Determined by Line Bundles, Divisors, and Linear Systems . . . . .	387
3	Fibrations Especially Surfaces Over Curves . . . . .	390
4	Generalities on Elliptic Fibrations of Surfaces Over Curves . . . . .	392
5	Elliptic K3 Surfaces . . . . .	395
6	Fibrations of 3 Dimensional Calabi–Yau Varieties . . . . .	397
7	Three Examples of Three Dimensional Calabi–Yau Hypersurfaces in Weight Projective Four Space and Their Fibrings . . . . .	400
	<b>Appendix I: Calabi–Yau Manifolds and String Theory . . . . .</b>	<b>403</b>
	<i>Stefan Theisen</i>	
	Why String Theory? . . . . .	403
	Basic Properties . . . . .	404
	String Theories in Ten Dimensions . . . . .	406
	Compactification . . . . .	407
	Duality . . . . .	409
	Summary . . . . .	411
	<b>Appendix II: Elliptic Curves in Algorithmic Number Theory and Cryptography . . . . .</b>	<b>413</b>
	<i>Otto Forster</i>	
1	Applications in Algorithmic Number Theory . . . . .	413
1.1	Factorization . . . . .	413
1.2	Deterministic Primality Tests . . . . .	415
2	Elliptic Curves in Cryptography . . . . .	417
2.1	The Discrete Logarithm . . . . .	417
2.2	Diffie–Hellman Key Exchange . . . . .	417
2.3	Digital Signatures . . . . .	418
2.4	Algorithms for the Discrete Logarithm . . . . .	419
2.5	Counting the Number of Points . . . . .	421
2.6	Schoof’s Algorithm . . . . .	421
2.7	Elkies Primes . . . . .	423
	References . . . . .	424



**Appendix III: Elliptic Curves and Topological Modular Forms** . . . . . 425

1 Categories in a Category . . . . . 427

2 Groupoids in a Category . . . . . 429

3 Cocategories over Commutative Algebras: Hopf Algebroids . . . . . 431

4 The Category  $WT(R)$  and the Weierstrass Hopf Algebroid . . . . . 434

5 Morphisms of Hopf Algebroids: Modular Forms . . . . . 438

6 The Role of the Formal Group in the Relation Between Elliptic  
Curves and General Cohomology Theory . . . . . 441

7 The Cohomology Theory or Spectrum  $tmf$  . . . . . 443

References . . . . . 444

**Appendix IV: Guide to the Exercises** . . . . . 445

*Ruth Lawrence*

**References** . . . . . 465

**List of Notation** . . . . . 479

**Index** . . . . . 481