

# 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](http://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

*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

© 2004 Springer Science+Business Media, 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 Science+Business Media, Inc., 233 Spring Street, New York, NY 10013, 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, service 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.

This reprint has been authorized by Springer-Verlag (Berlin/Heidelberg/New York) for sale in the Mainland China only and not for export therefrom.

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 Weierstrasse 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 beginning 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.



---

## 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

<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

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>	<b>57</b>
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>	<b>65</b>
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>	<b>85</b>
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>	<b>103</b>
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>	<b>125</b>
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

<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