

Cambridge University Press

978-0-521-65817-1 - Elliptic Curves: Function Theory, Geometry, Arithmetic

Henry McKean and Victor Moll

Frontmatter

[More information](#)

---

The subject of elliptic curves is one of the jewels of nineteenth-century mathematics, originated by Abel, Gauss, Jacobi, and Legendre. This book presents an introductory account of the subject in the style of the original discoverers, with references to and comments about more recent and modern developments. The treatment combines three of the fundamental themes of mathematics: complex function theory, geometry, and arithmetic.

After an informal preparatory chapter on rational functions, Riemann surfaces, and the like, the book follows a historical path, beginning with practical examples of elliptic integrals and the discovery of Abel and Gauss that the inversion of such an integral yields an elliptic function. This is followed by chapters on Jacobi's theta functions, modular groups and modular functions, Abel's and Hermite's work on the quintic, Kronecker and Weber's imaginary quadratic field, and the Mordell–Weil theorem on the rational points of elliptic curves.

Requiring only a first acquaintance with complex function theory, this book is an ideal introduction to the subject for students of mathematics and physics. The many exercises with hints scattered throughout the text give the reader a glimpse of further developments.

Cambridge University Press

978-0-521-65817-1 - Elliptic Curves: Function Theory, Geometry, Arithmetic

Henry McKean and Victor Moll

Frontmatter

[More information](#)

---

## ELLIPTIC CURVES

Cambridge University Press

978-0-521-65817-1 - Elliptic Curves: Function Theory, Geometry, Arithmetic

Henry McKean and Victor Moll

Frontmatter

[More information](#)

# ELLIPTIC CURVES

Function Theory, Geometry, Arithmetic

HENRY McKEAN

*New York University*

VICTOR MOLL

*Tulane University*



Cambridge University Press

978-0-521-65817-1 - Elliptic Curves: Function Theory, Geometry, Arithmetic  
Henry McKean and Victor Moll

Frontmatter

[More information](#)

PUBLISHED BY THE PRESS SYNDICATE OF THE UNIVERSITY OF CAMBRIDGE  
The Pitt Building, Trumpington Street, Cambridge, United Kingdom

CAMBRIDGE UNIVERSITY PRESS  
The Edinburgh Building, Cambridge CB2 2RU, United Kingdom  
40 West 20th Street, New York, NY 10011-4211, USA  
10 Stamford Road, Oakleigh, Melbourne 3166, Australia

© Henry McKean and Victor Moll 1999

This book is in copyright. Subject to statutory exception  
and to the provisions of relevant collective licensing agreements,  
no reproduction of any part may take place without  
the written permission of Cambridge University Press.

First published 1997

First paperback edition 1999 (with corrections)

Printed in the United States of America

Typeset in Times

*Library of Congress Cataloging-in-Publication Data*

McKean, Henry P.

Elliptic curves : function theory, geometry, arithmetic / Henry  
McKean, Victor Moll.

p. cm.

Includes bibliographical references.

1. Curves, Elliptic. I. Moll, Victor. II. Title.

QA567.2.E44M38 1997 96-36605  
516.3'52 - dc20 CIP

A catalog record for this book is available from  
the British Library.

ISBN 0 521 58228 8 hardback

ISBN 0 521 65817 9 paperback

Cambridge University Press

978-0-521-65817-1 - Elliptic Curves: Function Theory, Geometry, Arithmetic

Henry McKean and Victor Moll

Frontmatter

[More information](#)

---

In Memory of GRETCHEN WARREN

To Lisa, Alexander, and Stefan

Cambridge University Press

978-0-521-65817-1 - Elliptic Curves: Function Theory, Geometry, Arithmetic

Henry McKean and Victor Moll

Frontmatter

[More information](#)

---

I have always an idea in my mind, a certain confused picture, which shows me, as in a dream, a better form than I have used; but I cannot grasp it and develop it. And even this idea is only on a middling plane. From this I conclude that the works of those rich and great minds of ancient days are very far beyond the utmost stretch of my hopes and imagination. Their writings not only satisfy me to the full, but astound me and strike me with wonder. I appreciate their beauty; I see, if not the whole, at least so much that I cannot possibly aspire to equal it. Whatever I undertake, I owe a sacrifice to the Graces, to obtain their favor. . . . But they always leave me in the lurch. With me everything is rough; there is a lack of grace, charm, and beauty. I am incapable of making things show for all that they are; my style adds nothing to the matter. That is why my subject must be a solid one, with plenty to grip, and one that shines with its own lustre.

Montaigne, *On Presumption*

Book 2, Chapter 17, *Essays*, trans. J. M. Cohen.

Penguin Classics. New York, 1958.

## Contents

<i>Preface</i>	<i>page xi</i>
<b>1. First Ideas: Complex Manifolds, Riemann Surfaces, and Projective Curves</b>	<b>1</b>
1.1 The Riemann Sphere	1
1.2 Complex Manifolds	3
1.3 Rational Functions	7
1.4 Luroth's Theorem	8
1.5 Automorphisms of $\mathbb{P}^1$	12
1.6 Spherical Geometry	14
1.7 Finite Subgroups and the Platonic Solids	16
1.8 Automorphisms of the Half-Plane	24
1.9 Hyperbolic Geometry	25
1.10 Projective Curves	27
1.11 Covering Surfaces	30
1.12 Scissors and Paste	33
1.13 Algebraic Functions	41
1.14 Examples	46
1.15 More on Uniformization	51
1.16 Compact Manifolds as Curves: Finale	52
<b>2. Elliptic Integrals and Functions</b>	<b>54</b>
2.1 Elliptic Integrals: Where They Come From	55
2.2 The Incomplete Integrals Reduced to Normal Form	62
2.3 The Complete Integrals: Landen, Gauss, and the Arithmetic–Geometric Mean	65
2.4 The Complete Elliptic Integrals: Legendre's Relation	68

Cambridge University Press

978-0-521-65817-1 - Elliptic Curves: Function Theory, Geometry, Arithmetic

Henry McKean and Victor Moll

Frontmatter

[More information](#)

viii	<i>Contents</i>	
2.5	The Discovery of Gauss and Abel	71
2.6	Periods in General	77
2.7	Elliptic Functions in General	81
2.8	The $\wp$ -Function	84
2.9	Elliptic Integrals, Complete and Incomplete	87
2.10	Two Mechanical Applications	89
2.11	The Projective Cubic	92
2.12	The Problem of Inversion	93
2.13	The Function Field	95
2.14	Addition on the Cubic	98
2.15	Abel's Theorem	104
2.16	Jacobian Functions: Reprise	109
2.17	Covering Tori	113
2.18	Finale: Higher Genus	118
<b>3.</b>	<b>Theta Functions</b>	<b>125</b>
3.1	Jacobi's Theta Functions	125
3.2	Some Identities	127
3.3	The Jacobi and Weierstrass Connections	131
3.4	Projective Embedding of Tori	133
3.5	Products	135
3.6	Sums of Two Squares	140
3.7	Sums of Four Squares	142
3.8	Euler's Identities: <i>Partitio Numerorum</i>	143
3.9	Jacobi's and Higher Substitutions	147
3.10	Quadratic Reciprocity	150
3.11	Ramanujan's Continued Fractions	154
<b>4.</b>	<b>Modular Groups and Modular Functions</b>	<b>159</b>
4.1	The Modular Group of First Level	159
4.2	The Modular Group of Second Level	160
4.3	Fundamental Cells	162
4.4	Generating the Groups	166
4.5	Gauss on Quadratic Forms	167
4.6	The Group of Anharmonic Ratios	169
4.7	Modular Forms	172
4.8	Eisenstein Sums	176
4.9	Absolute Invariants	177
4.10	Triangle Functions	183



Cambridge University Press

978-0-521-65817-1 - Elliptic Curves: Function Theory, Geometry, Arithmetic

Henry McKean and Victor Moll

Frontmatter

[More information](#)

<i>Contents</i>	ix
4.11 The Modular Equation of Level 2	185
4.12 Landen's Transformation	187
4.13 Modular Equations of Higher Level	189
4.14 Jacobi's Modular Equation	192
4.15 Jacobi and Legendre's Derivation: Level 5	198
4.16 Arithmetic Subgroups: Overview	200
<b>5. <i>Ikosaeder</i> and the Quintic</b>	<b>206</b>
5.1 Solvability of Equations of Degree $\leq 4$	206
5.2 Galois Groups Revisited	207
5.3 The Galois Group of Level 5	209
5.4 An Element of Degree 5	212
5.5 Hermite on the Depressed Equation	214
5.6 Hermite on the Quintic	216
5.7 A Geometric View	217
<b>6. Imaginary Quadratic Number Fields</b>	<b>224</b>
6.1 Algebraic Numbers	225
6.2 Primes and Ideal Numbers	227
6.3 Class Invariants and Kronecker's <i>Jugendtraum</i>	235
6.4 Application of the Modular Equation	237
6.5 The Class Polynomial	239
6.6 Class Invariants at a Prime Level	243
6.7 Irreducibility of the Class Polynomial	248
6.8 Class Field and Galois Group	249
6.9 Computation of the Class Invariants	250
<b>7. Arithmetic of Elliptic Curves</b>	<b>252</b>
7.1 Arithmetic of the Projective Line	252
7.2 Cubics: The Mordell–Weil Theorem	253
7.3 Examples	255
7.4 Proof of the Mordell–Weil Theorem	259
<i>References</i>	265
<i>Index</i>	278

Cambridge University Press

978-0-521-65817-1 - Elliptic Curves: Function Theory, Geometry, Arithmetic

Henry McKean and Victor Moll

Frontmatter

[More information](#)

## Preface

The subject of **elliptic curves** such as  $y^2 = (1 - x^2)(1 - k^2x^2)$ , with  $k^2 \neq 0, 1$ , and of the corresponding **elliptic integrals**  $\int_0^x y^{-1} dx$  and the **elliptic functions** which invert them, is one of the jewels of nineteenth-century mathematics. Abel, Gauss, Jacobi, and Legendre are the masters here. It is a subject that combines in the most attractive way three of the fundamental themes of mathematics: complex function theory, geometry, and arithmetic. Naturally, it is possible to emphasize just one of these, but that we think is to miss the point, and so we have tried to keep a fair balance among them.

Chapter 1 is preparatory: It deals with rational functions, fractional linear substitutions, projective curves, Riemann surfaces, coverings, and the like, emphasizing low genus 0 or 1, but with glimpses of the higher genera  $g = 2$  or more. The presentation is often informal, but what is not actually proved is made plausible, and we thought it better to give a bird's-eye view of the fundamental facts than to get too much involved in the necessary technicalities.

Chapter 2 begins with practical examples of elliptic integrals and the discovery of Abel and Gauss that the inversion of such an integral yields an **elliptic function**, that is, a function of rational character on a complex torus produced by taking the complex plane  $\mathbb{C}$  modulo a lattice  $\mathbb{L} = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ . The remarkable geometric fact emerges that the class of elliptic curves  $\mathbf{X}$ , such as  $y^2 = (1 - x^2)(1 - k^2x^2)$ , and the class of complex tori are one and the same; in particular,  $\mathbf{X}$  carries a law of addition of rational character. The general discussion is mostly in the style of Weierstrass, though Jacobi's viewpoint is also explained and that of Legendre is sometimes preferred. The development is illustrated by occasional mechanical and other applications.

Chapter 3 is occupied by Jacobi's **theta functions**. These are not functions on the complex torus  $\mathbf{X} = \mathbb{C}/\mathbb{L}$  but rather on its universal cover  $\mathbb{C}$ , obeying simple transformation rules:  $\vartheta(x + 1) = \vartheta(x)$ ,  $\vartheta(x + \omega) = f\vartheta(x)$  with a factor  $f = e^{a+bx}$ . The subject is developed only so far as to permit several striking

Cambridge University Press

978-0-521-65817-1 - Elliptic Curves: Function Theory, Geometry, Arithmetic  
Henry McKean and Victor Moll

Frontmatter

[More information](#)

xii

*Preface*

geometric and arithmetic applications, such as the projective embedding of complex tori, counting the number of representations of a whole number as the sum of two squares, and the spectacular continued fractions of Ramanujan.

Chapter 4 is devoted to the **modular group**  $\Gamma_1 = PSL(2, \mathbb{Z})$  and some of its simpler arithmetic subgroups, and to the fundamental cells and absolute invariants attached to them. Quick explanations: Two complex tori are conformally equivalent if and only if their **period ratios**  $\omega = \omega_2/\omega_1$  are related by the action  $\omega \mapsto (a\omega + b)/(c\omega + d)^{-1}$  of a  $2 \times 2$  integer matrix  $[ab/cd]$  of determinant 1. These substitutions form the group  $\Gamma_1$ . The period ratio  $\omega$  is taken in the upper half-plane, so the quotient of the latter by  $\Gamma_1$  is a list of conformally inequivalent tori. Dedekind's **absolute invariant** of  $\Gamma_1$  supplies numbers: It is a function  $j$  of rational character in the period ratio  $\omega$  of  $\mathbf{X}$ , distinguished by the fact that two such curves  $\mathbf{X}$  are conformally equivalent if and only if their absolute invariants match. The Jacobi modulus  $k^2$ , viewed as a function of the period ratio, fills the same office of absolute invariant for the modular group  $\Gamma_2$  of second level comprised of modular substitutions congruent to the identity modulo 2. The highpoint is the **modular equation** relating the absolute invariants of two elliptic curves one of which covers the other. This part stems from Abel, Gauss, and Jacobi and has extraordinary arithmetic applications.

Abel proved that the general quintic is not solvable by radicals. Hermite discovered that the extra ingredient required is, so to speak, a single new "radical," namely, the eighth root of the Jacobi modulus  $k^2$ , in terms of which the roots of the modular equation of level 5 may be expressed. Chapter 5 explains this tour de force.

Chapter 6 tells the even more remarkable story, due to Kronecker and Weber, of the **class field** of the imaginary quadratic field  $\mathbb{Q}(\sqrt{D})$  for a square-free whole number  $D < 0$ . The class field is the biggest (unramified) extension of  $\mathbb{Q}(\sqrt{D})$  with commutative Galois group and is produced from  $\mathbb{Q}(\sqrt{D})$  in the most surprising manner: by the adjunction of certain class invariants  $j(\omega)$  attached to the integral ideals of  $\mathbb{Q}(\sqrt{D})$ . The modular equation plays a central role in this development, too.

Chapter 7 provides a glimpse of the arithmetic of elliptic curves per se; it is devoted to the theorem of Mordell and Weil stating that the rational points of such curves form a module of finite rank over  $\mathbb{Z}$ .

**Prerequisites.** Not much is needed besides a first acquaintance with complex function theory: primarily, Cauchy's theorem, Liouville's theorem, power series, residues, and such. Copson [1935], Hurwitz and Courant [1964], or Ahlfors [1979] would be fine; each of these contains, as well, a nice presentation of elliptic functions from the viewpoint of complex function theory,

Cambridge University Press

978-0-521-65817-1 - Elliptic Curves: Function Theory, Geometry, Arithmetic

Henry McKean and Victor Moll

Frontmatter

[More information](#)*Preface*

xiii

covering part of Chapters 2 and 3. A first acquaintance with the topology of curves and surfaces and with algebraic number fields and Galois theory would be helpful, but is not really necessary. What is needed is reviewed on the spot and you can either believe it or look it up.

Exercises with occasional hints are placed throughout the text. Please take them as an important part of the discussion and do them faithfully. It will pay off.

**Acknowledgments.** It is a pleasure to thank the audiences at MIT (1958–66), Rockefeller University (1966–9), NYU (1969–82) [H. McKean], and Tulane [V. Moll] (1986,1994) who have listened patiently while we learned the subject. Now one cannot remember who objected to this or clarified that, but any teacher will know how much we owe to them. It is an additional and very particular pleasure to thank P. Sarnak who has kindly read the whole book, with particular attention to the arithmetic parts, and corrected a number of mistakes and misapprehensions. The text owes its elegant appearance to the expertise of Meredith Mickel and the superb copyediting by G. M. Schreiber. The partial support of the National Science Foundation (summers 1981,1994 under grant nos. NSF-MCS 7900813 [H. McKean] and LEQSF(1991–4)-RD-A-31 [V. Moll] is gratefully acknowledged, too.

So. Landaff and New York  
New Orleans

*Henry McKean*  
*Victor Moll*