

# Elliptic Curves

Anthony W. Kasper

*Mathematical Notes 29*

PRINCETON UNIVERSITY PRESS

PRINCETON, NEW JERSEY

1973



# Elliptic Curves

by

Anthony W. Knapp

*Mathematical Notes 40*

PRINCETON UNIVERSITY PRESS

---

PRINCETON, NEW JERSEY

1992

Copyright © 1992 by Princeton University Press  
ALL RIGHTS RESERVED

The Princeton Mathematical Notes are edited by  
Luis A. Caffarelli, John N. Mather, and Elias M. Stein

Princeton University Press books are printed on acid-free  
paper, and meet the guidelines for permanence and durabil-  
ity of the Committee on Production Guidelines for Book  
Longevity of the Council on Library Resources

Printed in the United States of America

**Library of Congress Cataloging-in-Publication Data**

Knapp, Anthony W.

Elliptic curves / by Anthony W. Knapp.

p. cm.—(Mathematical notes ; 40)

Includes bibliographical references and index.

ISBN 0-691-08559-5 (PB)

1. Curves, Elliptic. I. Title. II. Series: Mathematical notes  
(Princeton University Press) ; 40.

QA567.2.E44K53 1993 516.3'52—dc20 92-22183

## CONTENTS

	List of Figures	v
	List of Tables	vii
	Preface	ix
	Standard Notation	xv
I.	Overview	1
II.	Curves and Projective Space	
	1. Projective Space	10
	2. Curves and Tangents	24
	3. Plane	32
	4. Applications to Cubics	37
	5. Projective Tangent and Osculating	44
III.	Class Groups of Number Fields	
	6. Z-Modules	50
	7. Weierstrass Form, Discriminant, Invariant	55
	8. Class Field	60
	9. Connections with Quadratic Fields	65
	10. The M-Process	70
IV.	Mordell's Theorem	
	11. Divisors	75
	12. Condition for Divisibility by $r$	80
	13. $\mathbb{Z}[Q]/\mathbb{Z}[Q]$ Special Cases	85
	14. $\mathbb{Z}[Q]/\mathbb{Z}[Q]$ , General Case	90
	15. Height and Mordell's Theorem	95
	16. Generalized Descent for Field	100
	17. Descent Based on the Rank	105
	18. Generalization of Descent to $\mathbb{Z}[Q]$	110
	19. Appendix on Algebraic Number Theory	115
V.	Torsion Subgroup of $\mathbb{Z}[Q]$	
	20. Overview	120
	21. Inductive Methods $r$	125
	22. Inductive Methods $r^2$	131
	23. Inductive Methods $r^3$	134
	24. Inductive Methods $r^4$	137
	25. Generalization of Descent with Polynomials	140
	26. Torsion Groups for General Curves	145



# CONTENTS

List of Figures	x
List of Tables	x
Preface	xi
Standard Notation	xv
I. Overview	3
II. Curves in Projective Space	
1. Projective Space	19
2. Curves and Tangents	24
3. Flexes	32
4. Application to Cubics	40
5. Bezout's Theorem and Resultants	44
III. Cubic Curves in Weierstrass Form	
1. Examples	50
2. Weierstrass Form, Discriminant, $j$ -invariant	56
3. Group Law	67
4. Computations with the Group Law	74
5. Singular Points	77
IV. Mordell's Theorem	
1. Descent	80
2. Condition for Divisibility by 2	85
3. $E(\mathbb{Q})/2E(\mathbb{Q})$ , Special Case	88
4. $E(\mathbb{Q})/2E(\mathbb{Q})$ , General Case	92
5. Height and Mordell's Theorem	95
6. Geometric Formula for Rank	102
7. Upper Bound on the Rank	107
8. Construction of Points in $E(\mathbb{Q})$	115
9. Appendix on Algebraic Number Theory	122
V. Torsion Subgroup of $E(\mathbb{Q})$	
1. Overview	130
2. Reduction Modulo $p$	134
3. $p$ -adic Filtration	137
4. Lutz-Nagell Theorem	144
5. Construction of Curves with Prescribed Torsion	145
6. Torsion Groups for Special Curves	148

VI.	Complex Points	
1.	Overview	151
2.	Elliptic Functions	152
3.	Weierstrass $\wp$ Function	153
4.	Effect on Addition	162
5.	Overview of Inversion Problem	165
6.	Analytic Continuation	166
7.	Riemann Surface of the Integrand	169
8.	An Elliptic Integral	174
9.	Computability of the Correspondence	183
VII.	Dirichlet's Theorem	
1.	Motivation	189
2.	Dirichlet Series and Euler Products	192
3.	Fourier Analysis on Finite Abelian Groups	199
4.	Proof of Dirichlet's Theorem	201
5.	Analytic Properties of Dirichlet $L$ Functions	207
VIII.	Modular Forms for $SL(2, \mathbf{Z})$	
1.	Overview	221
2.	Definitions and Examples	222
3.	Geometry of the $q$ Expansion	227
4.	Dimensions of Spaces of Modular Forms	231
5.	$L$ Function of a Cusp Form	238
6.	Petersson Inner Product	241
7.	Hecke Operators	242
8.	Interaction with Petersson Inner Product	250
IX.	Modular Forms for Hecke Subgroups	
1.	Hecke Subgroups	256
2.	Modular and Cusp Forms	261
3.	Examples of Modular Forms	265
4.	$L$ Function of a Cusp Form	267
5.	Dimensions of Spaces of Cusp Forms	271
6.	Hecke Operators	273
7.	Oldforms and Newforms	283
X.	$L$ Function of an Elliptic Curve	
1.	Global Minimal Weierstrass Equations	290
2.	Zeta Functions and $L$ Functions	294
3.	Hasse's Theorem	296



XI. Eichler-Shimura Theory	
1. Overview	302
2. Riemann surface $X_0(N)$	311
3. Meromorphic Differentials	312
4. Properties of Compact Riemann Surfaces	316
5. Hecke Operators on Integral Homology	320
6. Modular Function $j(\tau)$	333
7. Varieties and Curves	341
8. Canonical Model of $X_0(N)$	349
9. Abstract Elliptic Curves and Isogenies	359
10. Abelian Varieties and Jacobian Variety	367
11. Elliptic Curves Constructed from $S_2(\Gamma_0(N))$	374
12. Match of $L$ Functions	383
XII. Taniyama-Weil Conjecture	
1. Relationships among Conjectures	386
2. Strong Weil Curves and Twists	392
3. Computations of Equations of Weil Curves	394
4. Connection with Fermat's Last Theorem	397
Notes	401
References	409
Index of Notation	419
Index	423

## LIST OF FIGURES

1.1	Method for obtaining $\mathbb{Q}$ solutions of $x^2 + y^2 = 1$	6
1.2	Newton's explanation of the Diophantus method	10
1.3	Chord-tangent composition rule	11
1.4	Group laws relative to different base points $O$	11
1.5	Negatives relative to the group law	12
1.6	Singular behavior	13
1.7	Graphs of $\mathbb{R}$ points of the elliptic curve $y^2 = P(x)$	14
3.1	Configuration for $(PP')(QQ') = (PQ)(P'Q')$	69
8.1	Fundamental domain for $SL(2, \mathbb{Z})$	228
8.2	Contour for calculating number of zeros	232
9.1	Fundamental domain for $\Gamma_0(2)$	260

## LIST OF TABLES

1.1	Values of $\prod'_{p \leq R} N(p)/p$ for $y^2 = x^3 + ax$	17
3.1	Some elliptic curves with small negative discriminant	64
3.2	Some elliptic curves with small positive discriminant	65
4.1	Image of $\varphi$ for $y^2 = x^3 - 4x$ with $x \notin \{-2, 0, 2\}$	111
4.2	Image of $\varphi$ for $y^2 = x^3 - 4x$ with $x \in \{-2, 0, 2\}$	111
4.3	Adjusted image of $\varphi$ for $y^2 = x^3 - 4x$	111
4.4	Image of $\varphi$ for $y^2 = x^3 - p^2x$ with $x \notin \{-p, 0, p\}$	113
4.5	Adjusted image of $\varphi$ for $y^2 = x^3 - p^2x$	113
4.6	Some primes $p \equiv 5 \pmod{8}$ that are congruent numbers	117
4.7	Effect on $E: y^2 = x^3 + 8x$ of Fermat's descent	121
5.1	Examples of torsion subgroups of $E(\mathbb{Q})$	133
10.1	Effect of an admissible change of variables	291
12.1	Conductors of some elliptic curves	391
12.2	Curves $X_0(N)$ of low genus	395

## PREFACE

For introductory purposes, an elliptic curve over the rationals is an equation  $y^2 = P(x)$ , where  $P$  is a monic polynomial of degree three with rational coefficients and with distinct complex roots.

The points on such a curve, together with a point at infinity, form an abelian group under a geometric definition of addition. Namely if we take two points on the curve and connect them by a line, the line will intersect the curve in a third point. The reflection of that third point in the  $x$ -axis is taken as the sum of the given points. The identity is the point at infinity. According to Mordell's Theorem, the abelian group of points on the curve with rational coordinates is finitely generated. A theorem of Lutz and Nagell describes the torsion subgroup completely, but the rank of the free abelian part is as yet not fully understood.

This is the essence of the basic theory of rational elliptic curves. The first five of the twelve chapters of this book give an account of this theory, together with many examples and number-theoretic applications. This is beautiful mathematics, of interest to people in many fields. Except for one small part of the proof of Mordell's Theorem, it is elementary, requiring only undergraduate mathematics. Accordingly the presentation avoids most of the machinery of algebraic geometry.

A related theory concerns elliptic curves over the complex numbers, or Riemann surfaces of genus one. This subject requires complex variable theory and is discussed in Chapter VI. It leads naturally to the topic of modular forms, which is the subject of Chapters VIII and IX.

But the book is really about something deeper, the twentieth-century discovery of a remarkable connection between automorphy and arithmetic algebraic geometry. This connection first shows up in the coincidence of  $L$  functions that arise from some very special modular forms ("automorphic"  $L$  functions) with  $L$  functions that arise from number theory ("arithmetic" or "geometric"  $L$  functions, also called "motivic"). Chapter VII introduces this theme. The automorphic  $L$  functions have manageable analytic properties, while the arithmetic  $L$  functions encode subtle number-theoretic information. The fact that the arithmetic  $L$  functions are automorphic enables one to bring a great deal of mathematics to bear on extracting the number-theoretic information from the  $L$  function.

The prototype for this phenomenon is the Riemann zeta function  $\zeta(s)$ , which should be considered as an arithmetic  $L$  function defined initially

for  $\operatorname{Re} s > 1$ . An example of subtle number-theoretic information that  $\zeta(s)$  encodes is the Prime Number Theorem, which follows from the nonvanishing of  $\zeta(s)$  for  $\operatorname{Re} s = 1$ . In particular, this property of  $\zeta(s)$  is a property of points  $s$  outside the initial domain of  $\zeta(s)$ . To get a handle on analytic properties of  $\zeta(s)$ , one proves that  $\zeta(s)$  has an analytic continuation and a functional equation. These properties are completely formal once one establishes a relationship between  $\zeta(s)$  and a theta function with known transformation properties. Establishing this relationship is the same as proving that  $\zeta(s)$  is an automorphic  $L$  function.

The main examples of Chapter VII are the Dirichlet  $L$  functions  $L(s, \chi)$ . These too are arithmetic  $L$  functions defined initially for  $\operatorname{Re} s > 1$ . They encode Dirichlet's Theorem on primes in arithmetic progressions, which follows from the nonvanishing of all  $L(s, \chi)$  at  $s = 1$ . As with  $\zeta(s)$ , the relevant properties of  $L(s, \chi)$  are outside the initial domain. Also as with  $\zeta(s)$ , one gets at the analytic continuation and functional equation of  $L(s, \chi)$  by identifying  $L(s, \chi)$  with an automorphic  $L$  function.

The examples at the level of Chapter VII are fairly easy. Further examples, generalizing the Dirichlet  $L$  functions in a natural way, arise in abelian class field theory, are well understood even if not easy, and will not be discussed in this book. The simplest  $L$  functions that are not well understood come from elliptic curves. An elliptic curve has a geometric  $L$  function  $L(s, E)$  initially defined for  $\operatorname{Re} s > \frac{3}{2}$ . An example conjecturally of the subtle information that  $L(s, E)$  encodes is the rank of the free abelian group of rational points on the curve. This rank is believed to be the order of vanishing of  $L(s, E)$  at  $s = 1$ . Once again, the relevant property of  $L(s, E)$  is outside the initial domain. To address the necessary analytic continuation, one would like to know that  $L(s, E)$  is an automorphic  $L$  function. Work of Eichler and Shimura provides a clue where to look for such a relationship. Eichler and Shimura gave a construction for passing from certain cusp forms of weight two for Hecke subgroups of the modular group to rational elliptic curves. Under this construction, the  $L$  function of the cusp form (which is an automorphic  $L$  function) equals the  $L$  function of the elliptic curve. The Taniyama-Weil Conjecture expects conversely that every elliptic curve arises from this construction, followed by a relatively simple map between elliptic curves. This conjecture appears to be very deep; a theorem of Frey, Serre, and Ribet says that it implies Fermat's Last Theorem. The final three chapters discuss these matters; the last two take for granted more mathematics than do the earlier chapters.

If the theme were continued beyond the twelve chapters that are here,

eventually it would lead to the Langlands program, which brings in representation theory on the automorphic side of this correspondence. As a representation theorist, I come to elliptic curves from the point of view of the Langlands program. Although the book neither uses nor develops any representation theory, elliptic curves do give the simplest case of the program where the correspondence of  $L$  functions is not completely understood. Furthermore representation-theoretic methods occasionally yield results about elliptic curves that seem inaccessible by classical methods. From my point of view, they are an appropriate place to begin to study and appreciate the Langlands program. A beginning guide to the literature in this area appears in the section of Notes at the end of the book.

This book grew out of a brilliant series of a half dozen lectures by Don Zagier at the Tata Institute of Fundamental Research in Bombay in January 1988. The book incorporates notes from parts of courses that I gave at SUNY Stony Brook in Spring 1989 and Spring 1990. The organization owes a great deal to Zagier's lectures, and I have reproduced a number of illuminating examples of his. I am indebted to Zagier for offering his series of lectures.

Much of the mathematics here can already be found in other books, even if it has not been assembled in quite this way. Some sections of this book follow sections of other books rather closely. Notable among these other books are Fulton [1989],\* Hartshorne [1977], Husemoller [1987], Lang [1976] and [1987], Ogg [1969a], Serre [1973a], Shimura [1971a], Silverman [1986], and Walker [1950]. The expository paper Swinnerton-Dyer and Birch [1975] was also especially helpful. Detailed acknowledgments of these dependences may be found in the section of Notes at the end.

In addition, I would like to thank the following people for help in various ways, some large and some small: H. Farkas, N. Katz, S. Kudla, R. P. Langlands, S. Lichtenbaum, H. Matumoto, C.-H. Sah, V. Schechtman, and R. Stingley. The type-setting was by  $\mathcal{A}\mathcal{M}\mathcal{S}\text{-}\mathcal{T}\mathcal{E}\mathcal{X}$ , and the Figures were drawn with Mathematica. Financial support in part was from the National Science Foundation in the form of grants DMS 87-23046 and DMS 91-00367.

A. W. Knapp  
January, 1992

---

\*A name followed by a bracketed year is an allusion to the list of References at the end of the book. The date is followed by a letter in case of ambiguity.



## STANDARD NOTATION

Item	Meaning
$\#S$ or $ S $	number of elements in $S$
$\emptyset$	empty set
$A^c$	$A$ complement
$n$ positive	$n > 0$
$\mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}$	integers, rationals, reals, complex numbers
$\operatorname{Re} z$	real part of $z$
$\operatorname{Im} z$	imaginary part of $z$
$O(1)$	bounded term
$o(1)$	term tending to 0
$\doteq$	approximately numerically equal
$\sim$	asymptotic to, with ratio tending to 1
$\mathbf{Z}_m$	integers modulo $m$
$a \equiv b \pmod{m}$	$m$ divides $a - b$
$a \mid b$	$a$ divides $b$
$\operatorname{GCD}(a, b)$	greatest common divisor
1	multiplicative identity
1 or $I$	identity matrix
$\dim V$	dimension of vector space
$V'$	dual of vector space
$\operatorname{End}_k(V)$	linear maps of vector space to itself
$GL(n, k)$	general linear group over a field $k$
$SL(2, \mathbf{R}), SL(2, \mathbf{Z})$	group of 2-by-2 matrices of determinant 1
$\operatorname{Tr} A$	trace of $A$
$A^{\operatorname{tr}}$	transpose of $A$
$R^\times$	multiplicative group of invertible elements
$\bar{k}$	algebraic closure of $k$
$[A : B]$	index of $B$ in $A$ , or degree of $A$ in $B$
$\operatorname{Aut}_k(K)$	automorphism group of $K$ fixing $k$
$\sum \oplus$	direct sum (for emphasis)
$\pi_1$	fundamental group

