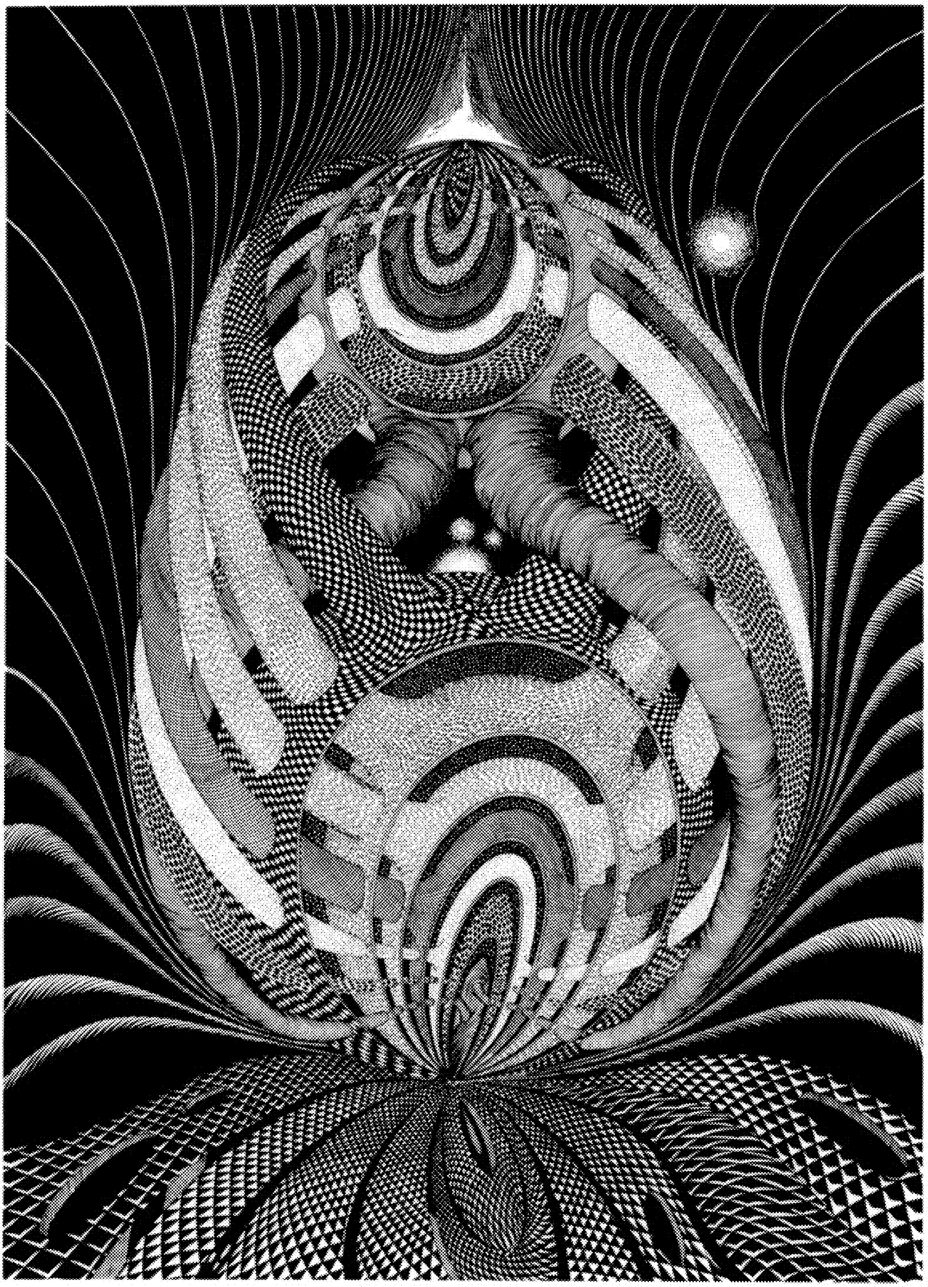
Graduate Texts in Mathematics 97

Springer-Science+Business Media, LLC



Neal Koblitz

Introduction to Elliptic Curves and Modular Forms

Second Edition

With 24 Illustrations

Springer

Neal Koblitz
Department of Mathematics
University of Washington
Seattle, WA 98195
USA

Mathematics Subject Classification (2000): 11-01, 11Dxx, 11Gxx, 11Rxx, 14H45

Library of Congress Cataloging-in-Publication Data
Koblitz, Neal.
Introduction to elliptic curves and modular forms / Neal Koblitz.
— 2nd ed.
p. cm. — (Graduate texts in mathematics; 97)
ISBN 978-1-4612-6942-7 ISBN 978-1-4612-0909-6 (eBook)
DOI 10.1007/978-1-4612-0909-6
1. Curves, Elliptic. 2. Forms, Modular. 3. Number Theory.
I. Title. II. Series.
QA567.2E44K63 1993
516.3′52—dc20 92-41778

Printed on acid-free paper.

Typeset by Asco Trade Typesetting Ltd., Hong Kong.

9 8 7 6 5 4

Preface to the First Edition

This textbook covers the basic properties of elliptic curves and modular forms, with emphasis on certain connections with number theory. The ancient "congruent number problem" is the central motivating example for most of the book.

My purpose is to make the subject accessible to those who find it hard to read more advanced or more algebraically oriented treatments. At the same time I want to introduce topics which are at the forefront of current research. Down-to-earth examples are given in the text and exercises, with the aim of making the material readable and interesting to mathematicians in fields far removed from the subject of the book.

With numerous exercises (and answers) included, the textbook is also intended for graduate students who have completed the standard first-year courses in real and complex analysis and algebra. Such students would learn applications of techniques from those courses, thereby solidifying their understanding of some basic tools used throughout mathematics. Graduate students wanting to work in number theory or algebraic geometry would get a motivational, example-oriented introduction. In addition, advanced undergraduates could use the book for independent study projects, senior theses, and seminar work.

This book grew out of lecture notes for a course I gave at the University of Washington in 1981–1982, and from a series of lectures at the Hanoi Mathematical Institute in April, 1983. I would like to thank the auditors of both courses for their interest and suggestions. My special gratitude is due to Gary Nelson for his thorough reading of the manuscript and his detailed comments and corrections. I would also like to thank Professors J. Buhler, B. Mazur, B. H. Gross, and Huynh Mui for their interest, advice and encouragement.

The frontispiece was drawn by Professor A. T. Fomenko of Moscow State University to illustrate the theme of this book. It depicts the family of elliptic curves (tori) that arises in the congruent number problem. The elliptic curve corresponding to a natural number n has branch points at 0, ∞, n and $-n$. In the drawing we see how the elliptic curves interlock and deform as the branch points $\pm n$ go to infinity.

Note: References are given in the form [Author year]; in case of multiple works by the same author in the same year, we use a, b, ... after the date to indicate the order in which they are listed in the Bibliography.

Seattle, Washington NEAL KOBLITZ

Preface to the Second Edition

The decade since the appearance of the first edition has seen some major progress in the resolution of outstanding theoretical questions concerning elliptic curves. The most dramatic of these developments have been in the direction of proving the Birch and Swinnerton-Dyer conjecture. Thus, one of the changes in the second edition is to update the bibliography and the discussions of the current state of knowledge of elliptic curves.

It was also during the 1980s that, for the first time, several important practical applications were found for elliptic curves. In the first place, the algebraic geometry of elliptic curves (and other algebraic curves, especially the curves that parametrize modular forms) were found to provide a source of new error-correcting codes which sometimes are better in certain respects than all previously known ones (see [van Lint 1988]). In the second place, H.W. Lenstra's unexpected discovery of an improved method of factoring integers based on elliptic curves over finite fields (see [Lenstra 1987]) led to a sudden interest in elliptic curves among researchers in cryptography. Further cryptographic applications arose as the groups of elliptic curves were used as the "site" of so-called "public key" encryption and key exchange schemes (see [Koblitz 1987], [Miller 1986], [Menezes and Vanstone 1990]).

Thus, to a much greater extent than I would have expected when I wrote this book, readers of the first edition came from applied areas of the mathematical sciences as well as the more traditional fields for the study of elliptic curves, such as algebraic geometry and algebraic number theory.

I would like to thank the many readers who suggested corrections and improvements that have been incorporated into the second edition.

Contents

CHAPTER III

CHAPTER IV