Elliptic Curves

Number Theory and Cryptography

Second Edition

© 2008 by Taylor & Francis Group, LLC

DISCRETE MATHEMATICS AND ITS APPLICATIONS

Series Editor
Kenneth H. Rosen, Ph.D.

Juergen Bierbrauer, Introduction to Coding Theory

Francine Blanchet-Sadri, Algorithmic Combinatorics on Partial Words

Kun-Mao Chao and Bang Ye Wu, Spanning Trees and Optimization Problems

Charalambos A. Charalambides, Enumerative Combinatorics

Henri Cohen, Gerhard Frey, et al., Handbook of Elliptic and Hyperelliptic Curve Cryptography

Charles J. Colbourn and Jeffrey H. Dinitz, Handbook of Combinatorial Designs, Second Edition

Martin Erickson and Anthony Vazzana, Introduction to Number Theory

Steven Furino, Ying Miao, and Jianxing Yin, Frames and Resolvable Designs: Uses, Constructions, and Existence

Randy Goldberg and Lance Riek, A Practical Handbook of Speech Coders

Jacob E. Goodman and Joseph O'Rourke, Handbook of Discrete and Computational Geometry, Second Edition

Jonathan L. Gross, Combinatorial Methods with Computer Applications

Jonathan L. Gross and Jay Yellen, Graph Theory and Its Applications, Second Edition

Jonathan L. Gross and Jay Yellen, Handbook of Graph Theory

Darrel R. Hankerson, Greg A. Harris, and Peter D. Johnson, Introduction to Information Theory and Data Compression, Second Edition

Daryl D. Harms, Miroslav Kraetzl, Charles J. Colbourn, and John S. Devitt, Network Reliability: Experiments with a Symbolic Algebra Environment

Leslie Hogben, Handbook of Linear Algebra

Derek F. Holt with Bettina Eick and Eamonn A. O'Brien, Handbook of Computational Group Theory

David M. Jackson and Terry I. Visentin, An Atlas of Smaller Maps in Orientable and Nonorientable Surfaces

Richard E. Klima, Neil P . Sigmon, and Ernest L. Stitzinger, Applications of Abstract Algebra with Maple™ and MATLAB® , Second Edition

Patrick Knupp and Kambiz Salari, Verification of Computer Codes in Computational Science and Engineering

© 2008 by Taylor & Francis Group, LLC

Continued Titles

William Kocay and Donald L. Kreher, Graphs, Algorithms, and Optimization

Donald L. Kreher and Douglas R. Stinson, Combinatorial Algorithms: Generation Enumeration and Search

Charles C. Lindner and Christopher A. Rodgers, Design Theory

Hang T. Lau, A Java Library of Graph Algorithms and Optimization

Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, Handbook of Applied Cryptography

Richard A. Mollin, Algebraic Number Theory

Richard A. Mollin, Codes: The Guide to Secrecy from Ancient to Modern Times

Richard A. Mollin, Fundamental Number Theory with Applications, Second Edition

Richard A. Mollin, An Introduction to Cryptography, Second Edition

Richard A. Mollin, Quadratics

Richard A. Mollin, RSA and Public-Key Cryptography

Carlos J. Moreno and Samuel S. Wagstaff, Jr., Sums of Squares of Integers

Dingyi Pei, Authentication Codes and Combinatorial Designs

Kenneth H. Rosen, Handbook of Discrete and Combinatorial Mathematics

Douglas R. Shier and K.T. Wallenius, Applied Mathematical Modeling: A Multidisciplinary Approach

Jörn Steuding, Diophantine Analysis

Douglas R. Stinson, Cryptography: Theory and Practice, Third Edition

Roberto Togneri and Christopher J. deSilva, Fundamentals of Information Theory and Coding Design

W. D. Wallis, Introduction to Combinatorial Designs, Second Edition

Lawrence C. Washington, Elliptic Curves: Number Theory and Cryptography, Second Edition

© 2008 by Taylor & Francis Group, LLC

DISCRETE MATHEMATICS AND ITS APPLICATIONS

Series Editor KENNETH H. ROSEN

ELLIPTIC CURVES
NUMBER THEORY AND CRYPTOGRAPHY

SECOND EDITION

LAWRENCE C. WASHINGTON
UNIVERSITY OF MARYLAND
COLLEGE PARK, MARYLAND, U.S.A.

Chapman & Hall/CRC
Taylor & Francis Group
Boca Raton London New York

Chapman & Hall/CRC is an imprint of the
Taylor & Francis Group, an **informa** business

© 2008 by Taylor & Francis Group, LLC

Chapman & Hall/CRC
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

© 2008 by Taylor & Francis Group, LLC
Chapman & Hall/CRC is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works
Printed in the United States of America on acid-free paper
10 9 8 7 6 5 4 3 2 1

International Standard Book Number-13: 978-1-4200-7146-7 (Hardcover)

This book contains information obtained from authentic and highly regarded sources Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The Authors and Publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, please access www.copyright.com (http://www.copyright.com/) or contact the Copyright Clearance Center, Inc. (CCC) 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Library of Congress Cataloging-in-Publication Data

Washington, Lawrence C.
Elliptic curves : number theory and cryptography / Lawrence C. Washington. -- 2nd ed.
p. cm. -- (Discrete mathematics and its applications ; 50)
Includes bibliographical references and index.
ISBN 978-1-4200-7146-7 (hardback : alk. paper)
1. Curves, Elliptic. 2. Number theory. 3. Cryptography. I. Title. II. Series.

QA567.2.E44W37 2008
516.3'52--dc22 2008006296

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

To Susan and Patrick

© 2008 by Taylor & Francis Group, LLC

Preface

Over the last two or three decades, elliptic curves have been playing an increasingly important role both in number theory and in related fields such as cryptography. For example, in the 1980s, elliptic curves started being used in cryptography and elliptic curve techniques were developed for factorization and primality testing. In the 1980s and 1990s, elliptic curves played an important role in the proof of Fermat's Last Theorem. The goal of the present book is to develop the theory of elliptic curves assuming only modest backgrounds in elementary number theory and in groups and fields, approximately what would be covered in a strong undergraduate or beginning graduate abstract algebra course. In particular, we do not assume the reader has seen any algebraic geometry. Except for a few isolated sections, which can be omitted if desired, we do not assume the reader knows Galois theory. We implicitly use Galois theory for finite fields, but in this case everything can be done explicitly in terms of the Frobenius map so the general theory is not needed. The relevant facts are explained in an appendix.

The book provides an introduction to both the cryptographic side and the number theoretic side of elliptic curves. For this reason, we treat elliptic curves over finite fields early in the book, namely in Chapter 4. This immediately leads into the discrete logarithm problem and cryptography in Chapters 5, 6, and 7. The reader only interested in cryptography can subsequently skip to Chapters 11 and 13, where the Weil and Tate-Lichtenbaum pairings and hyperelliptic curves are discussed. But surely anyone who becomes an expert in cryptographic applications will have a little curiosity as to how elliptic curves are used in number theory. Similarly, a non-applications oriented reader could skip Chapters 5, 6, and 7 and jump straight into the number theory in Chapters 8 and beyond. But the cryptographic applications are interesting and provide examples for how the theory can be used.

There are several fine books on elliptic curves already in the literature. This book in no way is intended to replace Silverman's excellent two volumes [109], [111], which are the standard references for the number theoretic aspects of elliptic curves. Instead, the present book covers some of the same material, plus applications to cryptography, from a more elementary viewpoint. It is hoped that readers of this book will subsequently find Silverman's books more accessible and will appreciate their slightly more advanced approach. The books by Knapp [61] and Koblitz [64] should be consulted for an approach to the arithmetic of elliptic curves that is more analytic than either this book or [109]. For the cryptographic aspects of elliptic curves, there is the recent book of Blake et al. [12], which gives more details on several algorithms than the

© 2008 by Taylor & Francis Group, LLC

present book, but contains few proofs. It should be consulted by serious students of elliptic curve cryptography. We hope that the present book provides a good introduction to and explanation of the mathematics used in that book. The books by Enge [38], Koblitz [66], [65], and Menezes [82] also treat elliptic curves from a cryptographic viewpoint and can be profitably consulted.

Notation. The symbols $\mathbf{Z}$, $\mathbf{F}_q$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ denote the integers, the finite field with q elements, the rationals, the reals, and the complex numbers, respectively. We have used $\mathbf{Z}_n$ (rather than $\mathbf{Z}/n\mathbf{Z}$) to denote the integers mod n. However, when p is a prime and we are working with $\mathbf{Z}_p$ as a field, rather than as a group or ring, we use $\mathbf{F}_p$ in order to remain consistent with the notation $\mathbf{F}_q$. Note that $\mathbf{Z}_p$ does not denote the p-adic integers. This choice was made for typographic reasons since the integers mod p are used frequently, while a symbol for the p-adic integers is used only in a few examples in Chapter 13 (where we use $\mathcal{O}_p$). The p-adic rationals are denoted by $\mathbf{Q}_p$. If K is a field, then $\overline{K}$ denotes an algebraic closure of K. If R is a ring, then $R^\times$ denotes the invertible elements of R. When K is a field, $K^\times$ is therefore the multiplicative group of nonzero elements of K. Throughout the book, the letters K and E are generally used to denote a field and an elliptic curve (except in Chapter 9, where K is used a few times for an elliptic integral).

Acknowledgments. The author thanks Bob Stern of CRC Press for suggesting that this book be written and for his encouragement, and the editorial staff at CRC Press for their help during the preparation of the book. Ed Eikenberg, Jim Owings, Susan Schmoyer, Brian Conrad, and Sam Wagstaff made many suggestions that greatly improved the manuscript. Of course, there is always room for more improvement. Please send suggestions and corrections to the author (lcw@math.umd.edu). Corrections will be listed on the web site for the book (www.math.umd.edu/∼lcw/ellipticcurves.html).

© 2008 by Taylor & Francis Group, LLC

Preface to the Second Edition

The main question asked by the reader of a preface to a second edition is "What is new?" The main additions are the following:

1. A chapter on isogenies.
2. A chapter on hyperelliptic curves, which are becoming prominent in many situations, especially in cryptography.
3. A discussion of alternative coordinate systems (projective coordinates, Jacobian coordinates, Edwards coordinates) and related computational issues.
4. A more complete treatment of the Weil and Tate-Lichtenbaum pairings, including an elementary definition of the Tate-Lichtenbaum pairing, a proof of its nondegeneracy, and a proof of the equality of two common definitions of the Weil pairing.
5. Doud's analytic method for computing torsion on elliptic curves over $\mathbf{Q}$.
6. Some additional techniques for determining the group of points for an elliptic curve over a finite field.
7. A discussion of how to do computations with elliptic curves in some popular computer algebra systems.
8. Several more exercises.

Thanks are due to many people, especially Susan Schmoyer, Juliana Belding, Tsz Wo Nicholas Sze, Enver Ozdemir, Qiao Zhang,and Koichiro Harada for helpful suggestions. Several people sent comments and corrections for the first edition, and we are very thankful for their input. We have incorporated most of these into the present edition. Of course, we welcome comments and corrections for the present edition (lcw@math.umd.edu). Corrections will be listed on the web site for the book (www.math.umd.edu/∼lcw/ellipticcurves.html).

© 2008 by Taylor & Francis Group, LLC

Suggestions to the Reader

This book is intended for at least two audiences. One is computer scientists and cryptographers who want to learn about elliptic curves. The other is for mathematicians who want to learn about the number theory and geometry of elliptic curves. Of course, there is some overlap between the two groups. The author of course hopes the reader wants to read the whole book. However, for those who want to start with only some of the chapters, we make the following suggestions.

Everyone: A basic introduction to the subject is contained in Chapters 1, 2, 3, 4. Everyone should read these.

I. Cryptographic Track: Continue with Chapters 5, 6, 7. Then go to Chapters 11 and 13.

II. Number Theory Track: Read Chapters 8, 9, 10, 11, 12, 14, 15. Then go back and read the chapters you skipped since you should know how the subject is being used in applications.

III. Complex Track: Read Chapters 9 and 10, plus Section 12.1.

© 2008 by Taylor & Francis Group, LLC

Contents

© 2008 by Taylor & Francis Group, LLC

© 2008 by Taylor & Francis Group, LLC

© 2008 by Taylor & Francis Group, LLC

© 2008 by Taylor & Francis Group, LLC