

Joseph H. Silverman

John Tate

Rational Points on Elliptic Curves

With 34 Illustrations



Springer

Joseph H. Silverman
Department of Mathematics
Brown University
Providence, RI 02912
USA

John Tate
Department of Mathematics
University of Texas at Austin
Austin, TX 78712
USA

Editorial Board

S. Axler
Mathematics Department
San Francisco State
University
San Francisco, CA 94132
USA

F.W. Gehring
Mathematics Department
East Hall
University of Michigan
Ann Arbor, MI 48109
USA

K.A. Ribet
Mathematics Department
University of California
at Berkeley
Berkeley, CA 94720-3840
USA

Mathematics Subject Classification (2000): 11G05, 11D25

Library of Congress Cataloging-in-Publication Data

Silverman, Joseph H., 1955–

Rational points on elliptic curves / Joseph H. Silverman, John Tate.

p. cm. — (Undergraduate texts in mathematics)

Includes bibliographical references and index.

ISBN 978-1-4419-3101-6

ISBN 978-1-4757-4252-7 (eBook)

DOI 10.1007/978-1-4757-4252-7

1. Curves, Elliptic. 2. Diophantine analysis. I. Tate, John Torrence, 1925– II. Title. III. Series.

QA567.2.E44S55 1992

516.3'52—dc20

92-4669

Printed on acid-free paper.

© 1992 Springer Science+Business Media New York

Originally published by Springer-Verlag New York Inc. in 1992

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, LLC), 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 of general descriptive names, trade names, trademarks, etc., in this publication, even if the former are not especially identified, is not to be taken as a sign that such names, as understood by the Trade Marks and Merchandise Marks Act, may accordingly be used freely by anyone.

Contents

Preface	v
Computer Packages	vii
Acknowledgments	vii
Introduction	1
CHAPTER I	
Geometry and Arithmetic	9
1. Rational Points on Conics	9
2. The Geometry of Cubic Curves	15
3. Weierstrass Normal Form	22
4. Explicit Formulas for the Group Law	28
Exercises	32
CHAPTER II	
Points of Finite Order	38
1. Points of Order Two and Three	38
2. Real and Complex Points on Cubic Curves	41
3. The Discriminant	47
4. Points of Finite Order Have Integer Coordinates	49
5. The Nagell-Lutz Theorem and Further Developments	56
Exercises	58
CHAPTER III	
The Group of Rational Points	63
1. Heights and Descent	63
2. The Height of $P + P_0$	68
3. The Height of $2P$	71
4. A Useful Homomorphism	76
5. Mordell's Theorem	83
6. Examples and Further Developments	89
7. Singular Cubic Curves	99
Exercises	102

CHAPTER IV

Cubic Curves over Finite Fields	107
1. Rational Points over Finite Fields	107
2. A Theorem of Gauss	110
3. Points of Finite Order Revisited	121
4. A Factorization Algorithm Using Elliptic Curves	125
Exercises	138

CHAPTER V

Integer Points on Cubic Curves	145
1. How Many Integer Points?	145
2. Taxicabs and Sums of Two Cubes	147
3. Thue's Theorem and Diophantine Approximation	152
4. Construction of an Auxiliary Polynomial	157
5. The Auxiliary Polynomial Is Small	165
6. The Auxiliary Polynomial Does Not Vanish	168
7. Proof of the Diophantine Approximation Theorem	171
8. Further Developments	174
Exercises	177

CHAPTER VI

Complex Multiplication	180
1. Abelian Extensions of \mathbb{Q}	180
2. Algebraic Points on Cubic Curves	185
3. A Galois Representation	193
4. Complex Multiplication	199
5. Abelian Extensions of $\mathbb{Q}(i)$	205
Exercises	213

APPENDIX A

Projective Geometry	220
1. Homogeneous Coordinates and the Projective Plane	220
2. Curves in the Projective Plane	225
3. Intersections of Projective Curves	233
4. Intersection Multiplicities and a Proof of Bezout's Theorem	242
5. Reduction Modulo p	251
Exercises	254
Bibliography	259
List of Notation	263
Index	267