

Serge Lang

Elliptic Curves Diophantine Analysis



Springer-Verlag Berlin Heidelberg GmbH 1978

Serge Lang

Department of Mathematics, Yale University,
New Haven, CT 06520, U.S.A.

AMS Subject Classification (1970): 10 B 45, 10 F 99, 14 G 25, 14 H 25

ISBN 978-3-642-05717-5 ISBN 978-3-662-07010-9 (eBook)
DOI 10.1007/978-3-662-07010-9

Library of Congress Cataloging in Publication Data. Lang, Serge, 1927–. Elliptic curves (Grundlehren der mathematischen Wissenschaften: 231). Bibliography: p. Includes index. 1. Diophantine analysis. 2. Curves, Elliptic. I. Title. II. Series: Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen; 231. QA242.L234. 512'.74. 77–21139.

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically those of translation, reprinting, re-use of illustrations, broadcasting, reproduction by photocopying machine or similar means, and storage in data banks. Under § 54 of the German Copyright Law where copies are made for other than private use, a fee is payable to the publisher, the amount of the fee to be determined by agreement with the publisher.

© by Springer-Verlag Berlin Heidelberg 1978

Originally published by Springer-Verlag Berlin Heidelberg New York in 1978

Typesetting: William Clowes & Sons Limited, London, Beccles and Colchester.

2141/3140–543210

Table of Contents

Part I. General Algebraic Theory

Chapter I. Elliptic Functions	3
§ 1. The Liouville Theorems.	3
§ 2. The Weierstrass Function	6
§ 3. The Addition Theorem	10
§ 4. Endomorphisms, Automorphisms, and Isomorphisms	13
§ 5. Points of Finite Order	17
§ 6. The Sigma and Zeta Function	19
§ 7. The Klein Form and the Siegel-Néron Function	23
§ 8. q -Expansions and Products	26
 Chapter II. The Division Equation	 33
§ 1. The Division Polynomial	33
§ 2. The Algebraic Formulas Over $\mathbf{Z}$	37
§ 3. Estimates for the Coefficients	43
 Chapter III. p-Adic Addition	 47
§ 1. Addition Near the Origin	48
§ 2. The Lutz-Nagell Theorem	54
§ 3. The Formal Group.	55
§ 4. The Néron Function	62
§ 5. The Tate Curve	68
§ 6. p -Adic Points of Order p	73
 Chapter IV. Heights	 77
§ 1. Basic Properties	77
§ 2. The Infinite Descent and Mordell-Weil Theorem	84
§ 3. Quasi-Linear Algebra.	85
§ 4. Quadraticity of the Height	88
§ 5. Linear Dependence of Algebraic Points	93
§ 6. Local Decomposition of the Height	98

Chapter V. Kummer Theory	101
§ 1. $A_K/2A_K$ is Finite	101
§ 2. The Kummer Pairing for Elliptic Curves	105
§ 3. Second Proof of the Weak Mordell–Weil Theorem	107
§ 4. Kummer Theory for the Multiplicative Group	109
§ 5. Bashmakov’s Theorem	115
 Chapter VI. Integral Points	128
§ 1. The Equation $ax + bx' = 1$ in Units	129
§ 2. Reduction of Integral Points to the Unit Equation by Siegel’s Method.	137
§ 3. Chabauty’s Method	140
§ 4. Reduction to the Weierstrass Form.	142
§ 5. The Thue–Siegel Curve	144
§ 6. Curves of Genus 0	146
§ 7. Applications to Curves of Higher Genus	147
§ 8. Reduction to Inequalities on Elliptic Logarithms	148
Appendix	151
 Part II. Approximation of Logarithms	
 Chapter VII. Auxiliary Results	159
§ 1. Heights and Sizes	159
§ 2. Linear Equations	162
§ 3. Estimates for Derivatives	164
§ 4. Feldman Polynomials	166
§ 5. Estimates for Entire Functions.	169
§ 6. The p -Adic Case.	173
Introduction to the Baker Method	176
 Chapter VIII. The Baker–Feldman Theorem	181
§ 1. Statement of the Theorem.	181
§ 2. Main Lemma and its Application	184
§ 3. Construction of the Approximating Function	186
§ 4. Two Estimates	188
§ 5. Extrapolation on Integral Multiples	190
§ 6. Extrapolation on Fractional Multiples	192

Chapter IX. Linear Combinations of Elliptic Logarithms 193

§ 1. Remarks on Complex Multiplication 193

§ 2. Statement of the Theorem. 197

§ 3. Main Lemma and its Application 198

§ 4. Construction of the Approximating Function 199

§ 5. Some Estimates 202

§ 6. Extrapolation on Integral Multiples 207

§ 7. Extrapolation on Fractional Multiples 210

Introduction to Chapters X and XI. 212

Chapter X. The Baker–Tijdeman Theorem 218

§ 1. Statement of the Theorem. 218

§ 2. Main Lemma and its Application 221

§ 3. Construction of the System of Linear Equations 226

§ 4. Extrapolation on Integral Multiples 229

§ 5. Extrapolation on Fractional Multiples 232

Chapter XI. Refined Inequalities 234

§ 1. Statement of the Theorem. 234

§ 2. Main Lemma and its Application 235

§ 3. Construction of the System of Linear Equations 238

§ 4. Proof of the Main Lemma 241

§ 5. Final Descent 246

Bibliography 253

Subject Index 260