Lecture Notes in Mathematics 1716

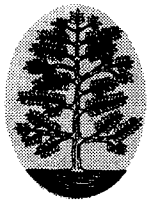
Springer
Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Singapore
Tokyo

J. Coates R. Greenberg
K. A. Ribet K. Rubin

Arithmetic Theory of Elliptic Curves

Lectures given at the 3rd Session of the Centro Internazionale Matematico Estivo (C.I.M.E.) held in Cetraro, Italy, July 12–19, 1997

Editor: C. Viola



Fondazione
C.I.M.E.

Springer

Authors

John H. Coates
Department of Pure Mathematics
and Mathematical Statistics
University of Cambridge
16 Mill Lane
Cambridge CB2 1SB, UK

Ralph Greenberg
Department of Mathematics
University of Washington
Seattle, WA 98195, USA

Kenneth A. Ribet
Department of Mathematics
University of California
Berkeley CA 94720, USA

Karl Rubin
Department of Mathematics
Stanford University
Stanford CA 94305, USA

Editor

Carlo Viola
Dipartimento di Matematica
Università di Pisa
Via Buonarroti 2
56127 Pisa, Italy

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Arithmetic theory of elliptic curves : held in Cetraro, Italy, July 12 - 19, 1997 / Fondazione CIME. J. Coates ... Ed.: C. Viola. - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 1999
(Lectures given at the ... session of the Centro Internazionale Matematico Estivo (CIME) ... ; 1997,3) (Lecture notes in mathematics ; Vol. 1716 : Subseries: Fondazione CIME)
ISBN 3-540-66546-3

Mathematics Subject Classification (1991):
11G05, 11G07, 11G15, 11G18, 11G40, 11R18, 11R23, 11R34, 14G10, 14G35

ISSN 0075-8434
ISBN 3-540-66546-3 Springer-Verlag Berlin Heidelberg New York

Printed in Germany

Typesetting: Camera-ready TEX output by the authors
SPIN: 10700270 41/3143-543210 - Printed on acid-free paper

Preface

The C.I.M.E. Session "Arithmetic Theory of Elliptic Curves" was held at Cetraro (Cosenza, Italy) from July 12 to July 19, 1997.

The arithmetic of elliptic curves is a rapidly developing branch of mathematics, at the boundary of number theory, algebra, arithmetic algebraic geometry and complex analysis. After the pioneering research in this field in the early twentieth century, mainly due to H. Poincaré and B. Levi, the origin of the modern arithmetic theory of elliptic curves goes back to L. J. Mordell's theorem (1922) stating that the group of rational points on an elliptic curve is finitely generated. Many authors obtained in more recent years crucial results on the arithmetic of elliptic curves, with important connections to the theories of modular forms and L-functions. Among the main problems in the field one should mention the Taniyama–Shimura conjecture, which states that every elliptic curve over $\mathbb{Q}$ is modular, and the Birch and Swinnerton–Dyer conjecture, which, in its simplest form, asserts that the rank of the Mordell–Weil group of an elliptic curve equals the order of vanishing of the L-function of the curve at 1. New impetus to the arithmetic of elliptic curves was recently given by the celebrated theorem of A. Wiles (1995), which proves the Taniyama–Shimura conjecture for semistable elliptic curves. Wiles' theorem, combined with previous results by K. A. Ribet, J.-P. Serre and G. Frey, yields a proof of Fermat's Last Theorem. The most recent results by Wiles, R. Taylor and others represent a crucial progress towards a complete proof of the Taniyama–Shimura conjecture. In contrast to this, only partial results have been obtained so far about the Birch and Swinnerton–Dyer conjecture.

The fine papers by J. Coates, R. Greenberg, K. A. Ribet and K. Rubin collected in this volume are expanded versions of the courses given by the authors during the C.I.M.E. session at Cetraro, and are broad and up-to-date contributions to the research in all the main branches of the arithmetic theory of elliptic curves. A common feature of these papers is their great clarity and elegance of exposition.

Much of the recent research in the arithmetic of elliptic curves consists in the study of modularity properties of elliptic curves over $\mathbb{Q}$, or of the structure of the Mordell–Weil group $E(K)$ of K-rational points on an elliptic curve E defined over a number field K. Also, in the general framework of Iwasawa theory, the study of $E(K)$ and of its rank employs algebraic as well as analytic approaches.

Various algebraic aspects of Iwasawa theory are deeply treated in Greenberg's paper. In particular, Greenberg examines the structure of the p-primary Selmer group of an elliptic curve E over a $\mathbb{Z}_p$-extension of the field K, and gives a new proof of Mazur's control theorem. Rubin gives a

detailed and thorough description of recent results related to the Birch and Swinnerton–Dyer conjecture for an elliptic curve defined over an imaginary quadratic field K, with complex multiplication by K. Coates' contribution is mainly concerned with the construction of an analogue of Iwasawa theory for elliptic curves without complex multiplication, and several new results are included in his paper. Ribet's article focuses on modularity properties, and contains new results concerning the points on a modular curve whose images in the Jacobian of the curve have finite order.

The great success of the C.I.M.E. session on the arithmetic of elliptic curves was very rewarding to me. I am pleased to express my warmest thanks to Coates, Greenberg, Ribet and Rubin for their enthusiasm in giving their fine lectures and for agreeing to write the beautiful papers presented here. Special thanks are also due to all the participants, who contributed, with their knowledge and variety of mathematical interests, to the success of the session in a very co-operative and friendly atmosphere.

Carlo Viola

Table of Contents