Complex Multiplication

This is a self-contained account of the state of the art in classical complex multiplication that includes recent results on rings of integers and applications to cryptography using elliptic curves. The author is exhaustive in his treatment, giving a thorough development of the theories of elliptic functions, modular functions and quadratic number fields and providing a concise summary of the results from class field theory. The main results are accompanied by numerical examples, equipping any reader with all the tools and formulae they need.

Topics covered include: the construction of class fields over quadratic imaginary number fields by singular values of the modular invariant j and Weber's tau-function; explicit construction of rings of integers in ray class fields and Galois module structure; the construction of cryptographically relevant elliptic curves over finite fields; proof of Berwick's congruences using division values of the Weierstrass-p function; and relations between elliptic units and class numbers.

Reinhard Schertz was Professor of Mathematics at the University of Augsburg in Germany until his retirement in 2008.

New Mathematical Monographs

All the titles listed below can be obtained from good booksellers or from Cambridge University Press. For a complete series listing, visit http://www.cambridge.org/uk/series/sSeries.asp?code=NMM

1 M. Cabanes and M. Enguehard *Representation Theory of Finite Reductive Groups*
2 J.B. Garnett and D.E. Marshall *Harmonic Measure*
3 P. Cohn *Free Ideal Rings and Localization in General Rings*
4 E. Bombieri and W. Gubler *Heights in Diophantine Geometry*
5 Y.J. Ionin and M.S. Shrikhande *Combinatorics of Symmetric Designs*
6 S. Berhanu, P.D. Cordaro and J. Hounie *An Introduction to Involutive Structures*
7 A. Shlapentokh *Hilbert's Tenth Problem*
8 G. Michler *Theory of Finite Simple Groups I*
9 A. Baker and G. Wüstholz *Logarithmic Forms and Diophantine Geometry*
10 P. Kronheimer and T. Mrowka *Monopoles and Three-Manifolds*
11 B. Bekka, P. de la Harpe and A. Valette *Kazhdan's Property (T)*
12 J. Neisendorfer *Algebraic Methods in Unstable Homotopy Theory*
13 M. Grandis *Directed Algebraic Topology*
14 G. Michler *Theory of Finite Simple Groups II*

Complex Multiplication

REINHARD SCHERTZ
Universität Augsburg

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore,
São Paulo, Delhi, Dubai, Tokyo

Cambridge University Press
The Edinburgh Building, Cambridge CB2 8RU, UK

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9780521766685

First published 2010

Printed in the United Kingdom at the University Press, Cambridge

A catalogue record for this publication is available from the British Library

Library of Congress Cataloging-in-Publication Data

Schertz, Reinhard, 1943–
Complex multiplication / Reinhard Schertz.
p. cm. – (New mathematical monographs; 15)
ISBN 978-0-521-76668-5 (Hardback)
1. Multiplication, Complex. I. Title. II. Series.
QA564.S294 2010
516.3′52–dc22
2009051874

ISBN 978-0-521-76668-5 Hardback

to Marlies

Contents

Cambridge University Press
978-0-521-76668-5 - Complex Multiplication
Reinhard Schertz
Frontmatter
More information

Preface

The aim of this book is to give an account of the state of the art in classical complex multiplication including, in particular, recent results on rings of integers and applications to cryptography using elliptic curves. All requisites needed about elliptic functions, modular functions and quadratic number fields are developed in this book and the results from class field theory are summarised in compact form. Further, most of the main results presented in the following chapters are accompanied by a plethora of numerical examples.† The reader interested in the application of the various explicit results will therefore find all the necessary tools in this book.

After the early results of Abel and Kronecker at the beginning of and mid nineteenth century, Weber at the start of the twentieth century gave the first systematic account of complex multiplication in his "Lehrbuch der Algebra III". The aim of this theory is to generate abelian extensions of quadratic imaginary number fields by values of elliptic functions and modular functions. Up until 1931 further accounts of the theory were given by Fricke (1916, 1922) and Fueter (1924, 1927). Finally, Hasse (1927) using class field theory that had developed in the meantime, presented a very short and elegant version of complex multiplication. His work contains the generation of ray class fields over a quadratic imaginary number field by singular values of the modular invariant j and Weber's τ function, using in the proof, besides class field theory, only the discriminant from the theory of elliptic functions. A more detailed exposition of the theory including a proof of the principal ideal theorem was provided by Deuring (1958). However, results on rings of integers had not been thus far obtained.

† I would like to thank the KANT group of TU Berlin headed by Michael Pohst for their help in computation by KASH (www.math.tu-berlin.de/kant).

Geometrically, in complex multiplication the generation of ray class fields over imaginary quadratic number fields is quite analogous to the construction of cyclotomic fields by roots of unity, which are torsion points of the unit circle. In complex multiplication the role of the unit circle is taken by a suitable elliptic curve E: the coefficients of E generate the Hilbert class field Ω, and the ray class fields are obtained by adjoining to Ω the x-coordinate of some torsion point of E. In view of this analogy one may pose the question whether it is possible to find explicit construction not only for the fields but also for their rings of integers as algebra or as Galois modules. Further, analogous to cyclotomic theory, one may ask for constructions of unit groups together with formulae for the class number. In fact, all this has been shown in the works of Leopoldt (1954, 1962) to be possible for cyclotomic fields. The solutions to these problems in complex multiplication form the central topics of this book. The following problems are treated in detail:

- Classical and simple generators for ring class fields and ray class fields
- Construction of rings of integers in ray class fields by explicit basis
- Galois module structure of these rings of integers including explicit construction of Galois generators and associated orders
- Construction of unit groups of maximal rank including their relation to class numbers
- Proof and generalisation of Berwick's congruences for the singular values of the modular invariant j

A recent application of complex multiplication described in this book is concerned with

- the construction cryptographically relevant elliptic curves over finite fields.

As shown in Chapter 9, the problem behind this construction is to find generating polynomials with small coefficients for abelian extensions of a quadratic imaginary number field. In contrast to cyclotomic theory, this is a non-trivial task, because the singular values of the modular invariant and the Weber τ function have minimal polynomials with astronomic coefficients.

Compared to cyclotomic theory the results obtained in complex multiplication, so far, seem complete. On the other hand there are numerous interesting questions concerning the generalisation to abelian varieties of higher dimension, for which a thorough understanding of complex multiplication is essential. These questions are in fact of very real interest because varieties of higher dimension can also be applied in cryptography. Such results can, for example, be found in the works of Weng (2001, 2003) for curves of genus 2 and 3. Conversely, the generalisation of the construction of class fields including results on the structure of rings of integers and class numbers remain unsolved. To obtain such results it may be useful to look at geometric analogies and analytic relations between cyclotomic fields with the unit circle of genus 0 and class fields of complex multiplication with their elliptic curves of genus 1 as described in Chapters 6 and 7 and to find such relations between curves of genus 1 and a higher genus.