Contributions in Mathematical and Computational Sciences 6

Gebhard Böckle
Gabor Wiese *Editors*

Computations with Modular Forms

Proceedings of a Summer School and Conference, Heidelberg, August/September 2011

MATCH

IWR

Springer

Contributions in Mathematical and Computational Sciences 6

Gebhard Böckle
Gabor Wiese *Editors*

Computations with Modular Forms

Proceedings of a Summer School and Conference, Heidelberg, August/September 2011

MATCH
IWR
Springer

Contributions in Mathematical and Computational Sciences • Volume 6

Editors
Hans Georg Bock
Willi Jäger
Otmar Venjakob

For further volumes:
www.springer.com/series/8861

Gebhard Böckle • Gabor Wiese
Editors

Computations with Modular Forms

Proceedings of a Summer School and Conference, Heidelberg, August/September 2011

Springer

Editors
Gebhard Böckle
Interdisciplinary Center for Scientific Computing
Universität Heidelberg
Heidelberg, Germany

Gabor Wiese
UR Mathématiques
FSTC
Université du Luxembourg
Luxembourg, Luxembourg

ISSN 2191-303X ISSN 2191-3048 (electronic)
Contributions in Mathematical and Computational Sciences
ISBN 978-3-319-03846-9 ISBN 978-3-319-03847-6 (eBook)
DOI 10.1007/978-3-319-03847-6
Springer Cham Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014931210

Mathematics Subject Classification (2010): 11F11, 11F33, 11F80, 11F67, 11Y16, 11Y35, 11F55, 11F75

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface to the Series

Contributions to Mathematical and Computational Sciences

Mathematical theories and methods and effective computational algorithms are crucial in coping with the challenges arising in the sciences and in many areas of their application. New concepts and approaches are necessary in order to overcome the complexity barriers particularly created by nonlinearity, high-dimensionality, multiple scales and uncertainty. Combining advanced mathematical and computational methods and computer technology is an essential key to achieving progress, often even in purely theoretical research.

The term mathematical sciences refers to mathematics and its genuine sub-fields, as well as to scientific disciplines that are based on mathematical concepts and methods, including sub-fields of the natural and life sciences, the engineering and social sciences and recently also of the humanities. It is a major aim of this series to integrate the different sub-fields within mathematics and the computational sciences, and to build bridges to all academic disciplines, to industry and other fields of society, where mathematical and computational methods are necessary tools for progress. Fundamental and application-oriented research will be covered in proper balance.

The series will further offer contributions on areas at the frontier of research, providing both detailed information on topical research, as well as surveys of the state-of-the-art in a manner not usually possible in standard journal publications. Its volumes are intended to cover themes involving more than just a single "spectral line" of the rich spectrum of mathematical and computational research.

The Mathematics Center Heidelberg (MATCH) and the Interdisciplinary Center for Scientific Computing (IWR) with its Heidelberg Graduate School of Mathematical and Computational Methods for the Sciences (HGS) are in charge of providing and preparing the material for publication. A substantial part of the material will be acquired in workshops and symposia organized by these institutions in topical areas of research. The resulting volumes should be more than just proceedings collecting papers submitted in advance. The exchange of information and the discussions during the meetings should also have a substantial influence on the contributions.

This series is a venture posing challenges to all partners involved. A unique style attracting a larger audience beyond the group of experts in the subject areas of specific volumes will have to be developed.

Springer Verlag deserves our special appreciation for its most efficient support in structuring and initiating this series.

Heidelberg University, Germany

Hans Georg Bock
Willi Jäger
Otmar Venjakob

Preface

This volume contains original research articles, survey articles and lecture notes related to the *Computations with Modular Forms 2011* Summer School and Conference that was held at the University of Heidelberg in August and September 2011. Organized by Gebhard Böckle, John Voight and Gabor Wiese, the Summer School and Conference were supported by the Mathematics Center Heidelberg (MATCH), the DFG priority program Algorithmic and Experimental Methods in Algebra, Geometry and Number Theory (SPP 1489) and the Number Theory Foundation.

The study of modular forms can be traced back to the work of Jakob Bernoulli and Leonhard Euler in the 18th century, in which certain theta functions appear. Later, in the 19th century, the concept of a modular form was formalized, and the term *Modulform* (modular form) seems to have been coined by Felix Klein. Whereas in the classical period modular forms were studied through function theoretic methods, a deep algebraic and algebro-geometric theory emerged in the 20th century. Moreover, spectacular links with objects from other disciplines were conjectured and some of these conjectures were recently proved. The link most well-known to the general public is the one between elliptic curves over the rationals and weight two newforms with rational coefficients, going under the name Taniyama-Shimura-Weil Conjecture: its partial proof by Andrew Wiles in 1995 made headlines since it implies the famous Fermat's Last Theorem. Currently, a whole framework of conjectural links between modular forms (and automorphic forms in various generalizations), representation theoretic objects and number theoretic ones is being developed, intensively studied, and partially proved, going under the names (p-adic) Langlands Program, Fontaine-Mazur Conjecture, (generalizations of) Serre's Modularity Conjecture, etc.

Modular forms, elliptic curves and related objects have proven to be very amenable to explicit computer calculations. Such calculations have played a very prominent role for many years in the building and refining of theory. For instance, the famous Birch and Swinnerton-Dyer conjecture, one of the seven Millennium Prize Problems of the Clay Mathematics Institute, was discovered through computer calculations in the early 1960s. At about the same time the Sato-Tate Conjecture was made, to which Sato was inspired through a numerical study, whereas Tate was apparently led to it by a theoretical reasoning. Also, concerning Serre's very influential modularity conjecture: it was some computer calculations of Mestre that led Serre to be "convinced to take the conjecture seriously" ("suffisant pour me convaincre que la conjecture méritait d'être prise au sérieux"[1]).

Nowadays, computer computations are standard for classical modular forms and can be done for instance using Sage. Implementations of Hilbert modular forms and others are included, for instance, in the computer algebra system Magma. It is impossible to list all research articles in which the authors have made use of Cremona's database of elliptic curves (developed since the end of the 1980s), Stein's database of modular forms, or the various modular forms and elliptic curves related functionality implemented in computer algebra systems. Needless to say, computational data is particularly useful in the development of the conjectural building encompassed in the Langlands Program and related conjectures. From a different, real-life applications oriented perspective, one cannot stress enough the role of algorithms for elliptic curves (and generalizations thereof) used in cryptography (smart cards, mobile phones, passport authentication, etc.).

The main focus of the Computation with Modular Forms 2011 Summer School and Conference was the development and application of algorithms in the field of modular and automorphic forms. The Summer School held prior to the Conference was aimed at young researchers and PhD students working or interested in this area.[2]

During the Summer School, lecture series were given by: Paul Gunnells, *Lectures on computing cohomology of arithmetic groups*, David Loeffler, *Computing with algebraic modular forms* and Robert Pollack, *Overconvergent modular symbols*, with two guest lectures by Henri Darmon. These three themes offer an introduction to modern algorithms including some theoretical background for computations of and with modular forms. In addition, the most basic and widely used algorithm, *modular symbols*, was briefly covered. The organizers would like to take this opportunity to thank again the speakers of the Summer School for their excellent presentations and their willingness to write notes that are included in these proceedings.

The research part of the Conference covered a wide range of themes related to computations with modular forms. Not all talks are included in this volume but also not all contributions to this volume were presented at the Conference. A number of articles are concerned with modular forms and related cohomology classes over imaginary quadratic fields, that is, the situation of Bianchi groups. Haluk Şengün surveys arithmetic aspects of Bianchi groups, particularly focussing on their cohomology, its computation and its partly conjectural arithmetic significance. For speeding up modular symbols calculations, Adam Mohamed explicitly describes Hecke operators on Manin symbols over imaginary quadratic fields in his article. In a higher generality, Dan Yasaki provides a survey on computing Hecke eigenclasses on the cohomology of Bianchi groups, GL_2 over totally real fields, totally complex quartic and mixed signature cubic fields, based on Voronoĭ-Köcher reduction theory

[1] Jean-Pierre Serre, *Sur les représentation modulaires de degré 2 de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. 54, no. 1, 1987, 179–230.

[2] See also http://www1.iwr.uni-heidelberg.de/conferences/modularforms11/.

and the Sharbly complex. Paul Gunnels provides general background on this theory in his lecture series. Also motivated by modular symbols over imaginary quadratic fields, John Cremona and M. T. Aranés provide algorithms for treating cusps and Manin symbols over arbitrary number fields.

Still in the realm of computing modular forms, Kevin Buzzard outlines an algorithm for calculating weight one cusp forms in characteristic zero and over finite fields and reports on computational findings. A talk at the Conference by George Schaeffer described further developments and extensions in this domain, which Schaeffer obtained in his PhD thesis. Other computations with classical modular forms appear in the work of John Voight and John Willis who describe an algorithm for series expansions of such forms around CM points. An algorithm for computing algebraic modular forms for certain rather general classical higher rank groups is treated in the work of Matthew Greenberg and John Voight using lattice methods, which has close links to the lecture series of David Loeffler. Finally, Alan Lauder describes some explicit calculations of triple product p-adic L-functions. It is related to the talks given by Henri Darmon that complemented the lecture series by Robert Pollack.

Other articles cover experimental and theoretical results: Explicit computations of modular forms led Panagiotis Tsaknias to discover a natural generalization of Maeda's conjecture on Galois orbits of newforms to higher levels, on which he reports in his article. Bartosz Naskręcki investigates congruences modulo prime powers between cusp forms and Eisenstein series theoretically and on the computer. Loïc Merel gives a description of the component group of the real points of modular Jacobians and addresses the computational question of how to determine whether complex conjugation in a modular mod 2 representation is trivial or not.

Acknowledgements This volume owes its existence foremost to the efforts of its authors and the participants of the Conference and the Summer School. We would like to thank them heartily for their contributions. We would also like to express our sincere thanks to Florian Nowak for typesetting the volume and MATCH for the financial support that made this possible.

Our special thanks go to John Voight, for without his help, this volume would not have turned out the way it did; besides co-organizing the Conference, he also did an enormous amount of editorial work, for which we are indebted and grateful.

Heidelberg, Germany — Gebhard Böckle
Luxembourg, Luxembourg — Gabor Wiese

Contents

Part I
Summer School

Lectures on Computing Cohomology of Arithmetic Groups

Paul E. Gunnells

Abstract Let $\mathbf{G}$ be the reductive $\mathbb{Q}$-group $R_{F/\mathbb{Q}}\mathrm{GL}_n$, where $F/\mathbb{Q}$ is a number field. Let $\Gamma \subset \mathbf{G}$ be an arithmetic group. We discuss some techniques to compute explicitly the cohomology of Γ and the action of the Hecke operators on the cohomology.

1 Introduction

This is a writeup of five lectures given at the summer school *Computations with modular forms*, Heidelberg, Germany, in August 2011. The course covered essentially all the material here, although I have made some corrections and modifications with the benefit of hindsight, and have taken the opportunity to elaborate the presentation. I've tried to preserve the informal nature of the lectures.

I thank the organizers for the opportunity to speak, and the participants of the summer school for a stimulating environment. I thank my collaborators Avner Ash, Mark McConnell, and Dan Yasaki, for many years of fun projects, and for all that they've taught me about this material. Thanks are also due to an anonymous referee, who carefully read the lectures and made many valuable suggestions. Finally, I thank the NSF for supporting the research described in these lectures.

2 Cohomology and Holomorphic Modular Forms

The goal of our lectures is to explain how to explicitly compute some automorphic forms via cohomology of arithmetic groups. Thus we begin by reviewing modular symbols and how they can be used to compute with holomorphic modular forms. For more details we refer to [Cre97, Ste07]. This material should be compared with that in Rob Pollack's lectures [Pol], which contains a different perspective on similar material.

P.E. Gunnells (✉)
Department of Mathematics and Statistics, University of Massachusetts, Amherst, MA 01003, USA
e-mail: gunnells@math.umass.edu

G. Böckle, G. Wiese (eds.), *Computations with Modular Forms*, Contributions in Mathematical and Computational Sciences 6, DOI 10.1007/978-3-319-03847-6_1,

Let $N \geq 1$ be an integer, and let $\Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$ be the subgroup of matrices that are upper-triangular mod N. Let $\mathfrak{H} \subset \mathbb{C}$ be the upper halfplane of all z with positive imaginary part. The group $\Gamma_0(N)$ acts on $\mathfrak{H}$ by fractional linear transformations:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}. \tag{2.1}$$

We let $Y_0(N)$ be the quotient $\Gamma_0(N)\backslash\mathfrak{H}$. Then $Y_0(N)$ is a smooth algebraic curve defined over $\mathbb{Q}$, called an *(open) modular curve*.

The curve $Y_0(N)$ is not compact, and there is a standard way to compactify it. Let $\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q})$, where we think of $\mathbb{P}^1(\mathbb{Q})$ as being $\mathbb{Q} \cup \{\infty\}$ with $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ and ∞ lying infinitely far up the imaginary axis. The points $\partial\mathfrak{H}^* = \mathfrak{H}^* \smallsetminus \mathfrak{H}$ are called *cusps*. The action of $\Gamma_0(N)$ extends to the cusps, and after endowing $\mathfrak{H}^*$ with an appropriate topology, the quotient $X_0(N) = \Gamma_0(N)\backslash\mathfrak{H}^*$ has the structure of a smooth projective curve over $\mathbb{Q}$. This is what most people call the *modular curve*.

By work of Eichler, Haberland, and Shimura, the cohomology of the spaces $Y_0(N)$ and $X_0(N)$ has connections with modular forms. These are holomorphic functions $f\colon \mathfrak{H} \to \mathbb{C}$ satisfying the transformation law

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z), \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N),$$

where $k \geq 1$ is a fixed integer; f is also required to satisfy a growth condition as z approaches any cusp. The space of such functions $M_k(N)$ is a finite-dimensional complex vector space with a subspace $S_k(N)$ of *cusp forms*: these are the f that undergo exponential decay as z approaches any cusp. There is a natural complement $\mathrm{Eis}_k(N)$ to $S_k(N)$, called the space of *Eisenstein series*. Then we have

$$H^1\big(Y_0(N); \mathbb{C}\big) \xrightarrow{\sim} S_2(N) \oplus \overline{S}_2(N) \oplus \mathrm{Eis}_2(N), \tag{2.2}$$

$$H^1\big(X_0(N); \mathbb{C}\big) \xrightarrow{\sim} S_2(N) \oplus \overline{S}_2(N). \tag{2.3}$$

For example, let $N = 11$. Then it is known that $\dim M_2(11) = 2$ and $\dim S_2(11) = 1$. The curve $X_0(11)$ has genus 1, which is consistent with (2.3). The complement of $Y_0(11)$ in $X_0(11)$ consists of two points. Thus $Y_0(11)$ deformation retracts onto a graph with one vertex and three loops. This implies $H^1(Y_0(11); \mathbb{C}) \simeq \mathbb{C}^3$, again consistent with (2.2).
We can say even more about (2.2)–(2.3):

- We don't have to limit ourselves to quotients by $\Gamma_0(N)$. Indeed, we can use other finite-index subgroups, such as the subgroup $\Gamma_1(N)$ of matrices congruent to $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$ modulo N, or the principal congruence subgroup $\Gamma(N)$ of matrices congruent to the identity modulo N.[1] We could also work with cocompact subgroups

[1] Throughout these lectures we only work with congruence subgroups. For $\mathrm{SL}_2(\mathbb{Z})$ this means any group containing $\Gamma(N)$ for some N.