Explicit computations with modular Galois representations

Bosman, J.G.

Citation

Bosman, J. G. (2008, December 15). *Explicit computations with modular Galois representations*. Retrieved from https://hdl.handle.net/1887/13364

Explicit computations with modular Galois representations

Proefschrift

ter verkrijging van
de graad van Doctor aan de Universiteit Leiden,
op gezag van Rector Magnificus prof. mr. P. F. van der Heijden,
volgens besluit van het College voor Promoties
te verdedigen op maandag 15 december 2008
klokke 13.45 uur

door

Johannes Gerardus Bosman

geboren te Wageningen
in 1979

Samenstelling van de promotiecommissie:

Promotor: prof. dr. S. J. Edixhoven (Universiteit Leiden)

Referent: prof. dr. W. A. Stein (University of Washington)

Overige leden: prof. dr. J.-M. Couveignes (Université de Toulouse 2)
prof. dr. J. Klüners (Heinrich-Heine-Universität Düsseldorf)
prof. dr. H. W. Lenstra, Jr. (Universiteit Leiden)
prof. dr. P. Stevenhagen (Universiteit Leiden)
prof. dr. J. Top (Rijksuniversiteit Groningen)
prof. dr. S. M. Verduyn Lunel (Universiteit Leiden)
prof. dr. G. Wiese (Universität Duisburg-Essen)

Explicit computations with modular Galois representations

THOMAS STIELTJES INSTITUTE
FOR MATHEMATICS

Johan Bosman, Leiden 2008

The research leading to this thesis was partly supported by NWO.

Contents

Preface

The area of modular forms is one of the many junctions in mathematics where several disciplines come together. Among these disciplines are complex analysis, number theory, algebraic geometry and representation theory, but certainly this list is far from complete. In fact, the phrase ‘modular form’ has no precise meaning since modular forms come in many types and shapes. In this thesis, we shall be working with classical modular forms of integral weight, which are known to be deeply linked with two-dimensional representations of the absolute Galois group of the field of rational numbers.

In the past decades an astonishing amount of research has been performed on the deep *theoretical* aspects of these modular Galois representations. The most well-known result that came out of this is the proof of Fermat’s Last Theorem by Andrew Wiles. This theorem states that for any integer $n > 2$, the equation $x^n + y^n = z^n$ has no solutions in positive integers x, y and z. The fact that at first sight this theorem seems to have nothing to do with modular forms at all witnesses the depth as well as the broad applicability of the theory of modular Galois representations. Another big result has been achieved, namely a proof of Serre’s conjecture by Chandrashekhar Khare, Jean-Pierre Wintenberger and Mark Kisin. Serre’s conjecture states that every continuous two-dimensional odd irreducible residual representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ comes from a modular form. This can be seen as a vast generalisation of Wiles’s result and in fact the proof also uses Wiles’s ideas.

On the other hand, research on the *computational* aspects of modular Galois representations is still in its early childhood. At the moment of writing this thesis there is very little literature on this subject, though more and more people are starting to perform active research in this field. This thesis is part of a project, led by Bas Edixhoven, that focuses on the computations of Galois representations associated to modular forms. The project has a theoretical side, proving computability and giving solid runtime analyses, and an explicit side, performing actual computations. The main contributors to the theoretical part of the project are, at this moment of writing, Bas Edixhoven, Jean-Marc Couveignes, Robin de Jong and Franz Merkl. A preprint version of their work, which will eventually be published as a volume of the Annals of Mathematics Studies, is available [28]. As the title of this thesis already suggests, we will be dealing with the explicit side of the project. In the explicit calculations we will make some guesses and base ourselves on unproven heuristics. However, we will use Serre’s conjecture to prove the correctness of our results afterwards.

The thesis consists of four chapters. In Chapter 1 we will recall the relevant parts of the theory of modular forms and Galois representations. It is aimed at a reader who hasn't studied this subject before but who wants to be able to read the rest of the thesis as well. Chapter 2 will be discussing computational aspects of this theory, with a focus on performing explicit computations. Chapter 3 consists of a published article that displays polynomials with Galois group $\mathrm{SL}_2(\mathbb{F}_{16})$, computed using the methods of Chapter 2. Explicit examples of such polynomials could not be computed by previous methods. Chapter 4 will appear in the final version of the manuscript [28]. In that chapter, we present some explicit results on mod ℓ representations for level one cusp forms. As an application, we improve a known result on Lehmer's non-vanishing conjecture for Ramanujan's tau function.

Notations and conventions

Throughout the thesis we will be using the following notational conventions. For each field k we fix an algebraic closure $\overline{k}$, keeping in mind that we can embed algebraic extensions of k into $\overline{k}$. Furthermore, for each prime number p, we regard $\overline{\mathbb{Q}}$ as a subfield of $\overline{\mathbb{Q}}_p$ and $\overline{\mathbb{F}}_p$ will be regarded as a fixed quotient of the integral closure of $\mathbb{Z}_p$ in $\overline{\mathbb{Q}}_p$. Furthermore, if λ is a prime of a local or global field, then $\mathbb{F}_\lambda$ will denote its residue field.