Enumerating Galois Representations in Sage

Craig Citro[1 2] and Alexandru Ghitza[3]

[1] Google, Seattle WA
[2] Department of Mathematics, University of Washington,
Box 354350, Seattle WA 98195-4350, USA,
craigcitro@gmail.com
[3] Department of Mathematics and Statistics, University of Melbourne,
Parkville VIC 3010, Australia,
aghitza@alum.mit.edu

Abstract. We present an algorithm for enumerating all odd semisimple two-dimensional mod p Galois representations unramified outside p. We also discuss the implementation of this algorithm in Sage and give a summary of the results we obtained[4].

Key words: Galois representations, Sage, modular forms.

1 Introduction

A great deal of arithmetic questions have found natural interpretations (and often, answers) within the realm of Galois representations and modular forms: such applications include Diophantine equations, quadratic forms, or the study of combinatorial-arithmetic objects such as partitions. In this context, it is of interest to dispose of computational tools for working with modular forms and Galois representations.

In this note, we focus on two-dimensional *Galois representations mod p*, i.e. continuous group homomorphisms

$$\rho\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_p) \ .$$

(More precisely, we consider such representations which are semisimple, unramified outside p, and odd. For the theoretical background, we refer the reader to Khare's survey [3] or to Edixhoven's paper [2].)

By Serre's conjecture, now a theorem of Khare-Wintenberger (see [4], [5]), these representations are closely related to modular forms (mod p) of level 1 which are eigenvectors for all the Hecke operators. If f is such a form, of weight k and eigenvalues (a_ℓ), then for all primes $\ell \neq p$ we have

$$\mathrm{charpoly}(\rho(\mathrm{Frob}_\ell)) = X^2 - a_\ell X + \ell^{k-1} \ ,$$

[4] The authors wish to thank Kevin Buzzard for providing several corrections and a significant improvement to Theorem 1, and the referees for suggesting improvements to the exposition.

where Frob_ℓ is a Frobenius element at ℓ inside $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

The *(Hecke) eigensystem* corresponding to a mod p eigenform f is the sequence (a_ℓ) of eigenvalues indexed by all primes $\ell \neq p$. The i-th *twist* of (a_ℓ) is by definition the eigensystem $\left(\ell^i a_\ell\right)$. We write $[a_\ell]$ for a finite truncation of (a_ℓ), where the cutoff point will be clear from the context.

Inspired by a remark of Khare[5], we have set out to enumerate all odd semisimple mod p representations which are unramified outside p. This corresponds to enumerating all the Hecke eigensystems which occur in spaces of level 1 modular forms mod p.

2 Description of the Algorithm

The starting point is a classical result in the theory of modular forms mod p (see Theorem 3.4 in [2]): every Hecke eigensystem occurs, up to twist, in weights less than or equal to $p+1$. Therefore it suffices to generate the spaces M_k for weights $4 \leq k \leq p+1$ and find all the eigenforms in them, which will produce all the Hecke eigensystems up to twist. This list may however contain duplicates; we investigate this question in detail in [1], where we prove

Theorem 1.

(a) Let f_1 and f_2 be eigenforms of weights $k_1, k_2 \leq p+1$. If f_1 and f_2 have the same eigensystem up to twist, then $k_1 + k_2 = p+1$ or $k_1 + k_2 = p+3$.
(b) Let f_1 and f_2 be eigenforms of weights related in one of the ways described in (a). If f_1 and f_2 do not have the same eigensystem up to twist, then this is detected by a prime $\ell \neq p$ satisfying $\ell \leq (p+1)/6$.

In the process of proving Theorem 1, we obtained the following lower bound, which improves the best known lower bound (due to Serre, see Sect. 8 in [3]) by a factor of two:

Theorem 2. *Let $p > 19$ be prime. The number of odd semisimple 2-dimensional Galois representations mod p which are unramified outside p is bounded below by $p(p-1)/2$.*

Algorithm: Enumerate Galois representations mod p up to twist

1. For $4 \leq k \leq p+1$:
   (a) Compute a basis for the space M_k.
   (b) Decompose the space into Hecke eigenspaces.
   (c) For each eigenform, compute the eigenvalue a_ℓ of T_ℓ for primes ℓ up to the bound from Theorem 1. Store $(k, [a_\ell])$.

[5] From Sect. 8 of [3]: "[. . .] there are only finitely many semisimple 2-dimensional mod p representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of bounded (prime-to-p Artin) conductor. *It will be of interest to get quantitative refinements of this.*"

2. Remove duplicates: given $(k_1, [a_\ell])$ and $(k_2, [b_\ell])$ such that $k_1 + k_2 = p + 1$ or $p + 3$, check whether $[b_\ell]$ is a twist of $[a_\ell]$.

This creates the list of equivalence classes (up to twist) of Hecke eigensystems mod p. It is now straightforward to apply the twist operation to each list element and generate the list of all Hecke eigensystems.

3 Sage Implementation and Results

Our task requires computing the action of Hecke operators on spaces of modular forms of high weight. Sage [8] offers several implementations of these spaces for arbitrary levels. We have initially used modular symbols over finite fields for generating the lists of eigenforms, but this method becomes quite slow as the weight increases. Restricting to level 1 allows us to take advantage of a much faster way of working with these spaces: the Victor Miller basis (see Sect. 2.3 in [7] for the properties and the algorithm Sage uses to compute this basis).

We then use one Hecke operator T_ℓ at a time to decompose the space M_k into eigenspaces. This requires (at most) the first $k/12$ primes ℓ (see the appendix of [6]).

We have run the Sage implementation of our algorithm for all primes up to 211 (see Table 1). Apart from keeping track of the number of equivalence classes of eigensystems and the total number of eigensystems, we save the list of equivalence classes; given this it is very easy to take twists and generate the entire list.

p	number	p	number	p	number	p	number	p	number	p	number
2	1	23	264	59	4234	97	19200	137	53992	179	119705
3	1	29	532	61	4800	101	21600	139	55752	181	124020
5	4	31	630	67	6237	103	22797	149	69264	191	145445
7	9	37	1044	71	7420	107	25546	151	71700	193	150144
11	35	41	1480	73	8136	109	27216	157	80340	197	160132
13	48	43	1701	79	10257	113	30240	163	90477	199	164637
17	112	47	2185	83	12054	127	42903	167	97276	211	196560
19	153	53	3172	89	14784	131	46735	173	108016		

Table 1. Number of Galois representations mod p

Khare guesses in [3] that the number of Galois representations of the type we are considering should be asymptotic to $p^3/48$. There are two phenomena that can contribute to the actual number being smaller than the guess: (i) the existence of "companion forms", which in our context appear as duplicate equivalence classes of eigenforms; (ii) the failure of "multiplicity one" for Hecke eigenvalues mod p, which results in some spaces M_k not contributing their dimension's worth of eigenforms. In the range of our computations, the actual number of representations stays very close to the best known upper bound[6], suggesting that the two phenomena are indeed quite rare. We expect this trend to be confirmed by further computations.

[6] For instance, for $p = 211$ the quotient between the actual number (196560) and the upper bound (196665) is about 0.9995.

References

1. Citro, C., Ghitza, A.: Computing level 1 Hecke eigensystems (mod p), preprint
2. Edixhoven, B.: The weight in Serre's conjectures on modular forms. Invent. Math. 109(3), 563–594 (1992)
3. Khare, C.: Modularity of Galois representations and motives with good reduction properties. J. Ramanujan Math. Soc. 22(1), 75–100 (2007)
4. Khare, C., Wintenberger, J.P.: Serre's modularity conjecture. I. Invent. Math. 178(3), 485–504 (2009), `http://dx.doi.org/10.1007/s00222-009-0205-7`
5. Khare, C., Wintenberger, J.P.: Serre's modularity conjecture. II. Invent. Math. 178(3), 505–586 (2009), `http://dx.doi.org/10.1007/s00222-009-0206-6`
6. Lario, J.C., Schoof, R.: Some computations with Hecke rings and deformation rings. Experiment. Math. 11(2), 303–311 (2002), `http://projecteuclid.org/getRecord?id=euclid.em/1062621223`, with an appendix by Amod Agashe and William Stein
7. Stein, W.: Modular forms, a computational approach, Graduate Studies in Mathematics, vol. 79. American Mathematical Society, Providence, RI (2007), with an appendix by Paul E. Gunnells
8. Stein, W., et al.: Sage Mathematics Software (Version 4.4.1). The Sage Development Team (2010), available from `http://www.sagemath.org`