Journal de Théorie des Nombres
de Bordeaux 00 (XXXX), 000–000

Computing the number of certain Galois representations mod p

par Tommaso Giorgio Centeleghe

Résumé. En utilisant le lien entre représentations galoisiennes et formes modulaires provenant de la Conjecture de Serre, nous calculons, pour tout premier $p \leq 2593$, une borne pour le nombre de classes d'isomorphismes des représentations galoisiennes de $\mathbf{Q}$ sur un $\overline{\mathbf{F}}_p$–espace vectoriel de dimension deux qui sont irréductibles, impaires, et non–ramifiées en dehors de p.

Abstract. Using the link between Galois representations and modular forms established by Serre's Conjecture, we compute, for every prime $p \leq 2593$, a lower bound for the number of isomorphism classes of Galois representation of $\mathbf{Q}$ on a two–dimensional vector space over $\overline{\mathbf{F}}_p$ which are irreducible, odd, and unramified outside p.

1. Introduction

Let p be a prime number and $\overline{\mathbf{F}}_p$ an algebraic closure of $\mathbf{F}_p$, the finite field with p elements. Let $G_{\mathbf{Q}}$ denote the absolute Galois group of $\mathbf{Q}$, with respect to the choice of an algebraic closure $\overline{\mathbf{Q}}$ of $\mathbf{Q}$. An important consequence of (the level one case of) Serre's Modularity Conjecture is the following finiteness theorem:

Theorem 1.1. *There are only finitely many isomorphism classes of continuous representations $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ that are irreducible, odd, and unramified outside p.*

Continuity in this context means that ρ has open kernel; compactness of $G_{\mathbf{Q}}$ implies that ρ has finite image, and there exists a finite extension $\mathbf{F}(\rho)$ of $\mathbf{F}_p$ for which a model of ρ over $\mathbf{F}(\rho)$ can be found. The statement obtained from Theorem 1.1 replacing $\overline{\mathbf{F}}_p$ by a finite subfield $\mathbf{F}$ was known to be true classically as a consequence of the Hermite–Minkowski Theorem. The point of Theorem 1.1 is that for every prime p one can find a finite subfield $\mathbf{F}$ of $\overline{\mathbf{F}}_p$ so that *all* the representations considered can be realized over $\mathbf{F}$.

Manuscrit reçu le 30 août 2010.

Let $R(p)$ denote the non–negative integer defined by Theorem 1.1. From the refined version of Serre's Conjecture one immediately sees that $R(p)$ is bounded from above by a function $U(p)$ that behaves like $p^3/48+O(p^2)$ (cf. §3, (3.1) and (3.2)). Professor Khare has raised the question of whether this upper bound gave the correct asymptotic of $R(p)$ (cf. [10], §8). In his University of Utah thesis the author conjectured a positive answer. The conjecture predicts that congruences modulo p between characteristic zero eigenforms of weight $k \leq p+1$ are "rare" and that, moreover, the mod p Galois representations of $\mathbf{Q}$ associated to classical cusp forms of level one tend to be irreducible and wildly ramified at p.

In the computations presented in this paper we collected for all primes $p \leq 2593$ a lower bound $L(p)$ of $R(p)$. Using the link between Galois representations and modular forms established by Serre's Conjecture, we computed $L(p)$ by estimating the number of systems of Hecke eigenvalues arising from modular forms mod p of level one and corresponding to Galois representations of $\mathbf{Q}$ that are irreducible. The method adopted is based on the analysis of a *single* Hecke operator T_n to deduce information about the mod p arithmetic of the *whole* Hecke ring $\mathbf{T}_k^0$ (cf. §3 Prop. 3.2). One of the limits of this approach is that for a given p we are not always able to compute the number of representations that are tamely ramified, we instead obtain an upper bound. It is this very fact which prevents us from computing the exact value of $R(p)$ in all cases (cf. §6). Craig Citro and Alexandru Ghitza considered the same computational project, the method they used for computing is however different (cf. [4]). All our computations have been performed using Magma (cf. [3]).

In section 2 standard results from the theory of modular forms and Galois representations that are needed in the sequel are recalled. Section 3 contains a detailed explanation of the method used for computing $L(p)$. Sections 4 and 5 provide the commutative algebra on which our method is based, they are independent of the rest of the paper. The table with our results appears in section 6; among other things, the reader will find there the values of $L(p)$ that we have collected and the value of the ratio $(U(p)-L(p))/p^2$, which shows a tendency to remain close to zero.

The work presented in this paper started within my thesis project, I would like to express my gratitude to professor Chandrashekhar Khare for suggesting this direction of research as well as for the invaluable attention that I have received from him. This paper benefitted from many interesting conversations and advice that I received from professors Gebhard Böckle and Gabor Wiese during the past year. I am grateful to them for their important help. I would like to thank professor Ulrich Görtz for letting me use the computer Pluto at the Institute for Experimental Mathematics in Essen for performing the computations. I want to thank Craig Citro,

who taught me much about computing with modular forms. I thank the anonymous referee of the paper for helpful comments and remarks that improved the exposition. Finally, the help of Panagiotis Tsaknias with the implementation of the algorithm and the production of the table was vital for me. I heartily thank him for his kindness and availability.

2. Generalities

In this preliminary section we adopt a very utilitarian point of view and recall all the results that we need from the theory of modular forms (both classical and mod p) and their associated mod p Galois representations. For more details on modular forms on $\mathrm{SL}_2(\mathbf{Z})$ and their Hecke operators the reader can consult [12] and [16]. For an exposition of classical theorems linking mod p modular forms to Galois representations, as well as some more recent important development, the papers [5] and [6] are beautiful references. We prefer not to say anything about Serre's Conjecture here. Instead, we will constantly keep this important theorem in the back of our mind as motivation for studying systems of Hecke eigenvalues arising from modular forms mod p.

Let M_k denote the space of classical modular forms of weight k on the group $\mathrm{SL}_2(\mathbf{Z})$, and let M_k^0 be its cuspidal subspace. Denote by $\mathrm{M}_k(\mathbf{Z})$ (resp. $\mathrm{M}_k^0(\mathbf{Z})$) the submodule of M_k (resp. M_k^0) given by forms f whose expansion at infinity has integer coefficients. It is a basic fact that these submodules define integral structures, meaning that the natural inclusions $\mathrm{M}_k(\mathbf{Z}) \subset \mathrm{M}_k$ and $\mathrm{M}_k^0(\mathbf{Z}) \subset \mathrm{M}_k^0$ induce isomorphisms $\mathrm{M}_k(\mathbf{Z}) \otimes \mathbf{C} \simeq \mathrm{M}_k$ and $\mathrm{M}_k^0(\mathbf{Z}) \otimes \mathbf{C} \simeq \mathrm{M}_k^0$. One way to see this is by first observing that M_k admits a $\mathbf{C}$–basis given by certain monomials in the Eisenstein series E_4 and E_6, whose expansions at infinity lie in $\mathbf{Q} \otimes \mathbf{Z}[[q]]$ (cf. [12], I Thm. 2.2 and X §3, or [16], VII §3 Cor. 2 and §4), and then conclude by arguing that the $\mathbf{Z}$–rank of $\mathrm{M}_k(\mathbf{Z})$ cannot exceed the dimension of M_k.

Let p be a prime number. Following [14], we define the space $\mathrm{M}_k(\mathbf{F}_p)$ of modular forms mod p of weight k on $\mathrm{SL}_2(\mathbf{Z})$ to be $\mathrm{M}_k(\mathbf{Z})/p\,\mathrm{M}_k(\mathbf{Z})$, similarly the cuspidal subspace is $\mathrm{M}_k^0(\mathbf{F}_p) = \mathrm{M}_k^0(\mathbf{Z})/p\,\mathrm{M}_k^0(\mathbf{Z})$. If $p > 3$, then these definitions agree with the geometric definitions à la Katz ([9], Theorem 1.8.2).

For an integer $n > 0$, the n–th Hecke operator on the space M_k^0 is denoted by T_n, without reference to the weight k. The Hecke operators all commute with each other, and if $\ell_1, \ldots, \ell_r$ are the primes dividing n, the operator T_n can be written as a polynomial in the $T_{\ell_1}, \ldots, T_{\ell_r}$ with coefficients in $\mathbf{Z}$ (cf. [16], VII §5).

By definition, the Hecke ring $\mathbf{T}_k^0$ is the subring of $\mathrm{End}_{\mathbf{C}}(\mathrm{M}_k^0)$ generated by all the operators T_n, for $n > 0$, and the Hecke algebra $(\mathbf{T}_k^0)_{\mathbf{C}}$ is the smallest $\mathbf{C}$–subalgebra of $\mathrm{End}_{\mathbf{C}}(\mathrm{M}_k^0)$ containing all the T_n's.

For every n, the operator T_n is a semi–simple endomorphism preserving the integral structure $\mathrm{M}_k^0(\mathbf{Z})$. Moreover, the algebra $(\mathbf{T}_k^0)_{\mathbf{C}}$ acts on M_k^0 with multiplicity one (cf. [16], VII §5). As a consequence of these two facts one can deduce the following:

Theorem 2.1. *There exist number fields K_i, for $1 \leq i \leq r$, with rings of integers O_i, and an injective ring homomorphism*

$$\theta_k : \mathbf{T}_k^0 \longrightarrow \prod_{1 \leq i \leq r} O_i$$

which has finite cokernel. The $\mathbf{Z}$–rank of $\mathbf{T}_k^0$ is equal to $\dim_{\mathbf{C}}(\mathrm{M}_k^0)$.

A *system of eigenvalues* arising from M_k^0 is a collection (a_ℓ) of complex numbers, indexed by all primes ℓ, so that there exists a nonzero form $f \in \mathrm{M}_k^0$ for which $T_\ell(f) = a_\ell f$, for all ℓ. One can show that there is a bijection between systems of eigenvalues arising from M_k^0 and $\mathrm{Hom}_{\mathrm{rings}}(\mathbf{T}_k^0, \mathbf{C})$.

If $\theta_{k,i} : \mathbf{T}_k^0 \to O_i$ denotes the composition of θ_k with the projection onto O_i, then all the systems of eigenvalues arising from M_k^0 are described by $(\sigma(\theta_{k,i}(T_\ell)))$, where $1 \leq i \leq r$ and $\sigma \in G_{\mathbf{Q}}$ is any element (each K_i is considered as a subfield of $\mathbf{C}$).

Let us remark that in all known examples r is equal to 1 and the systems of eigenvalues arising from M_k^0 form a unique Galois orbit. Maeda's conjecture is the statement that this happens for all k.

The Hecke ring $\mathbf{T}_k^0$ acts naturally on the space $\mathrm{M}_k^0(\mathbf{F}_p)$ and, by extension of scalars, on $\mathrm{M}_k^0(\mathbf{F}_p) \otimes \overline{\mathbf{F}}_p$, denoted by $\mathrm{M}_k^0(\overline{\mathbf{F}}_p)$ in what follows. A *system of eigenvalues mod p* arising from $\mathrm{M}_k^0(\overline{\mathbf{F}}_p)$ is a collection $\Phi = (a_\ell)_{\ell \neq p}$ of elements $a_\ell \in \overline{\mathbf{F}}_p$, indexed by primes $\ell \neq p$, so that there exists a nonzero form $f \in \mathrm{M}_k^0(\overline{\mathbf{F}}_p)$ with $T_\ell(f) = a_\ell f$.

If $\Phi = (a_\ell)_{\ell \neq p}$ is any system of eigenvalues mod p, one can find a nonzero form $f \in \mathrm{M}_k^0(\overline{\mathbf{F}}_p)$ giving rise to Φ that is an eigenvector for T_p. Therefore there is a ring homomorphism $\lambda_\Phi : \mathbf{T}_k^0 \to \overline{\mathbf{F}}_p$ defined by $T(f) = \lambda_\Phi(T) f$, for $T \in \mathbf{T}_k^0$. The p–th eigenvalue a_p, and hence the morphism λ_Φ, is not unique in general, for this reason we have preferred to not include it in the definition of eigensystem mod p. However, it can be shown that uniqueness holds when the weight is not too large with respect to p:

Proposition 2.1. *If $k \leq 2p - 1$ then there is a natural bijection between mod p systems of eigenvalues arising from $\mathrm{M}_k^0(\overline{\mathbf{F}}_p)$ and the set of $\overline{\mathbf{F}}_p$–valued points of $\mathrm{Spec}(\mathbf{T}_k^0)$.*

By a classical result of Eichler, Shimura and Deligne, to any mod p system of eigenvalues Φ one can attach a continuous, semi–simple Galois representation

$$\rho_\Phi : G_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(\overline{\mathbf{F}}_p),$$

which is odd, unramified outside p, and that is characterized by the equalities

$$\text{tr}(\rho_\Phi(\text{Frob}_\ell)) = a_\ell, \quad \det(\rho_\Phi(\text{Frob}_\ell)) = \ell^{k-1}, \tag{2.1}$$

for all primes $\ell \neq p$, where Frob_ℓ is a Frobenius element of $G_{\mathbf{Q}}$ at ℓ (cf. [6], §11 Prop. 11.1).

If $h \in \mathbf{Z}_{\geq 0}$ is a nonnegative integer then it follows from the theory of the θ–operator on mod p modular forms (cf. [6], §4) that the collection $(\ell^h a_\ell)_{\ell \neq p}$ is a system of eigenvalues arising from $\text{M}^0_{k+h(p+1)}(\overline{\mathbf{F}}_p)$, denoted by $\Phi^{(h)}$. We have

$$\rho_{\Phi^{(h)}} \simeq \chi_p^h \otimes \rho_\Phi,$$

where $\chi_p : G_{\mathbf{Q}} \to \mathbf{F}_p^*$ is the mod p cyclotomic character, and $\Phi^{(h)}$ is usually called the h–fold twist of Φ.

The following theorem is due to Tate and Serre. It has been generalized to higher levels by Jochnowitz (cf. [8]) and Ash–Stevens (cf. [2]).

Theorem 2.2. *If Φ is a system of mod p eigenvalues arising from $\text{M}^0_k(\overline{\mathbf{F}}_p)$, then there exists a twist $\Phi^{(h)}$ that arises from $\text{M}^0_{k'}(\overline{\mathbf{F}}_p)$, where $2 \leq k' \leq p+1$.*

In the weight range $2, 3, \ldots, p+1$, and when ρ_Φ is irreducible, a theorem of Deligne (cf. [6], §12, Prop. 12.1) and one of Fontaine (cf. [5], §2 Thm. 2.6 and §6) say that the semi–simplification of the local representation $(\rho_\Phi)_p$, obtained by restricting ρ_Φ to a decomposition subgroup $D_p < G_{\mathbf{Q}}$ at p, is determined on the inertia subgroup by the (unique) eigenvalue a_p associated to Φ. We only point out that $a_p \neq 0$ if and only if $(\rho_\Phi)_p$ is reducible.

Let Φ be a system of eigenvalues mod p, and assume that ρ_Φ is irreducible. Since we are working with modular forms of level one, the local representation $(\rho_\Phi)_p$ *is* ramified and one observes that $(\rho_\Phi)_p$ is semi–simple if and only if it is tamely ramified. There is the following criterion for deciding when this happens:

Theorem 2.3. *Let Φ be a system of eigenvalues arising from $\text{M}^0_k(\overline{\mathbf{F}}_p)$, where $2 \leq k \leq p+1$, and so that ρ_Φ is irreducible. Then $(\rho_\Phi)_p$ is tamely ramified if and only if one of the following mutually exclusive conditions holds:*

i) $\Phi^{(2-k)}$ arises from $\text{M}^0_{p+3-k}(\overline{\mathbf{F}}_p)$;

ii) $\Phi^{(1-k)}$ arises from $\text{M}^0_{p+1-k}(\overline{\mathbf{F}}_p)$.

From the description of $(\rho_\Phi)_p$ given by the theorems of Deligne and Fontaine mentioned above, and from an elementary analysis of the θ–cycle of Φ (cf. [7]), one sees that part i) in Theorem 2.3 is equivalent to $(\rho_\Phi)_p$ being irreducible. In the *much* harder case when $(\rho_\Phi)_p$ is reducible, the

criterion was conjectured by Serre and proved by Gross (cf. [6], §13 Thm. 13.10).

3. Computations

Let p be any prime number, and let $\mathcal{E}^{\mathrm{Irr}}(p)$ be the set of all systems $\Phi = (a_\ell)_{\ell \neq p}$ of Hecke eigenvalues mod p arising from $\mathrm{M}_k^0(\overline{\mathbf{F}}_p)$, for some k, so that the associated Galois representation ρ_Φ is irreducible. By the level one case of Serre's Conjecture, proved by Khare in 2005 (cf. [11]), the cardinality of $\mathcal{E}^{\mathrm{Irr}}(p)$ is equal to the integer $R(p)$ defined in the Introduction.

According to Theorem 2.2, any eigensystem Φ admits a twist in the weight range $2 \leq k \leq p+1$. Since the number of systems of eigenvalues mod p arising from M_k^0 is bounded from above by $\dim_{\overline{\mathbf{F}}_p}(\mathrm{M}_k^0(\overline{\mathbf{F}}_p)) = \dim_{\mathbf{C}}(\mathrm{M}_k^0)$, we have the following inequality

$$R(p) = |\mathcal{E}^{\mathrm{Irr}}(p)| \leq (p-1) \sum_{2 \leq k \leq p+1} \dim_{\mathbf{C}}(\mathrm{M}_k^0). \tag{3.1}$$

Let $U(p)$ be the upper bound for $R(p)$ given by inequality (3.1). Using the well–known formulas for $\dim_{\mathbf{C}}(\mathrm{M}_k^0)$ (cf. [12], p. 12), one finds that there is an explicit degree 3 polynomial $F_\alpha(x) \in \mathbf{Q}[x]$, depending only on the residue class α of p mod 12, and unique if $\alpha \neq 2, 3$ mod 12, so that $F_\alpha(p) = U(p)$ for all $p \in \alpha$. Letting p grow to infinity, one finds that

$$U(p) \sim p^3/48 + O(p^2). \tag{3.2}$$

Professor Khare has raised the question of whether this estimate gave the correct asymptotic behaviour with p of $R(p)$ (cf. [10], §8), in his thesis the author was led to conjecture a positive answer. The difficulty of this conjecture is producing lower bounds for $R(p)$. In this direction, the best result known today is due to Serre, who showed in an unpublished correspondence with Khare that $R(p)$ is bounded from below by a function of the type $cp^2 + O(p)$, for a constant $c > 0$ (cf. also [4]).

In our computations, for all primes $p \leq 2593$, we obtain a lower bound $L(p)$ for $R(p)$. The values of $L(p)$ are displayed in the fifth column of the table of section 6 next to the ratio $(U(p) - L(p))/p^2$, appearing in the sixth column. In the range explored this ratio is close to zero, showing a tendency for $R(p)$ to approach $U(p)$. For several primes p, we found that $L(p)$ is the actual value of $R(p)$; to highlight this, $L(p)$ appears starred in the table. These primes p are precisely those for which our computations revealed the non–existence of mod p representations of the type considered that are tamely ramified at p and of non–dihedral type (cf. §3.3 for more details).

We proceed to explain in detail how we computed $L(p)$. Since $U(p) = 0$ for $p < 11$, from now on p will be a prime ≥ 11. Part of the theoretical basis of the method is provided by the commutative algebra explained in

sections 4 and 5 of the paper. We adopt here some of the notation there established; so that, for example, δ_R denotes the discriminant of a finite $S_{\mathbf{Q}}$–ring R (cf. §4).

Let k be an even integer in the range $2, 4, \ldots, p+1$, and let $\mathcal{E}(p,k)$ be the set of mod p systems of Hecke eigenvalues Φ appearing in the space $\mathrm{M}_k^0(\overline{\mathbf{F}}_p)$. Consider the following subsets of $\mathcal{E}(p,k)$, defined in terms of the Galois representation ρ_Φ associated to Φ:

$\mathcal{E}^{\mathrm{Eis}}(p,k) = \{\Phi \in \mathcal{E}(p,k) \mid \rho_\Phi \text{ is reducible}\}$;
$\mathcal{E}^{p-\mathrm{tame}}(p,k) = \{\Phi \in \mathcal{E}(p,k) - \mathcal{E}^{\mathrm{Eis}}(p,k) \mid (\rho_\Phi)_p \text{ is tamely ramified}\}$;
$\mathcal{E}^{p-\mathrm{wild}}(p,k) = \{\Phi \in \mathcal{E}(p,k) - \mathcal{E}^{\mathrm{Eis}}(p,k) \mid (\rho_\Phi)_p \text{ is wildly ramified}\}$;
$\mathcal{E}^{p-\mathrm{split}}(p,k) = \{\Phi \in \mathcal{E}(p,k) - \mathcal{E}^{\mathrm{Eis}}(p,k) \mid (\rho_\Phi)_p \text{ is decomposable}\}$;
$\mathcal{E}^{p-\mathrm{irr}}(p,k) = \{\Phi \in \mathcal{E}(p,k) - \mathcal{E}^{\mathrm{Eis}}(p,k) \mid (\rho_\Phi)_p \text{ is irreducible}\}$.

Notice that there are the following disjoint unions (cf. section 2):

$$\mathcal{E}(p,k) = \mathcal{E}^{\mathrm{Eis}}(p,k) \cup \mathcal{E}^{p-\mathrm{tame}}(p,k) \cup \mathcal{E}^{p-\mathrm{wild}}(p,k),$$

$$\mathcal{E}^{p-\mathrm{tame}}(p,k) = \mathcal{E}^{p-\mathrm{split}}(p,k) \cup \mathcal{E}^{p-\mathrm{irr}}(p,k).$$

Moreover, for $k \leq p+1$, there are natural bijections

$$\mathcal{E}^{p-\mathrm{irr}}(p,k) \ni \Phi \longleftrightarrow \Phi^{(2-k)} \in \mathcal{E}^{p-\mathrm{irr}}(p, p+3-k),$$

$$\mathcal{E}^{p-\mathrm{split}}(p,k) \ni \Phi \longleftrightarrow \Phi^{(1-k)} \in \mathcal{E}^{p-\mathrm{split}}(p, p+1-k).$$

From Theorem 2.3 we deduce the formula

$$|\mathcal{E}^{\mathrm{Irr}}(p)| = (p-1) \sum_{2 \leq k \leq p+1} \left[|\mathcal{E}(p,k)| - |\mathcal{E}^{\mathrm{Eis}}(p,k)| - \frac{1}{2} |\mathcal{E}^{p-\mathrm{tame}}(p,k)| \right] \tag{3.3}$$

For all primes $p \leq 2593$ and all weights $k \leq p+1$, we managed to compute the values of $|\mathcal{E}(p,k)|$ and $|\mathcal{E}^{\mathrm{Eis}}(p,k)|$ (cf. §3.1, §3.2). On the other hand we obtained only an upper bound for $|\mathcal{E}^{p-\mathrm{tame}}(p,k)|$ (cf §3.3). This resulted in producing the lower bound $L(p)$ of $|\mathcal{E}^{\mathrm{Irr}}(p)| = R(p)$ we were looking for.

3.1. Computation of $|\mathcal{E}^{\mathrm{Eis}}(p,k)|$. This is the simplest quantity to compute, at least when $k \leq p+1$, thanks to the following criterion:

Proposition 3.1. *Let p be a prime and $k \leq p+1$ an integer so that $\mathrm{M}_k^0(\mathbf{F}_p) \neq 0$. Then $\mathcal{E}^{\mathrm{Eis}}(p,k)$ is not empty if and only if p divides the numerator of the k–th Bernoulli number b_k. Moreover, if $\mathcal{E}^{\mathrm{Eis}}(p,k)$ is not empty then it consists only of the mod p eigensystem $\Phi(E_k) = (1 + \ell^{k-1})_{\ell \neq p}$.*

Proof. A possible proof can be carried out using a filtration argument. The details can be found in ([14], §3.2 i)), where a proof in the case $k < p-1$ is given. The proof there extends to the cases $k \leq p+1$, mainly thanks to the fact that $\mathrm{M}_p^0(\mathbf{F}_p) = 0$. □

3.2. Computation of $|\mathcal{E}(p,k)|$. Let k be a weight $\leq p+1$, and n_k the integer $\dim_{\overline{\mathbf{F}}_p}(\mathrm{M}_k^0(\overline{\mathbf{F}}_p)) = \dim_{\mathbf{C}}(\mathrm{M}_k^0)$. Instead of computing directly $|\mathcal{E}(p,k)|$, we find it convenient to compute the difference $n_k - |\mathcal{E}(p,k)|$ between the number of characteristic zero eigensystems arising from M_k^0 and that of mod p eigensystems arising from the same space. Such integer can be considered as a measure of the occurrence of mod p congruences between eigenforms in M_k^0. The method used is described in the following application of Proposition 5.1 from section 5:

Proposition 3.2. *Let r be a positive integer, $T_r \in \mathbf{T}_k^0$ the r–th Hecke operator, and $h_r(x) \in \mathbf{Z}[x]$ its characteristic polynomial as an endomorphism of $\mathrm{M}_k^0(\mathbf{C})$. Assume that the discriminant δ_r of $h_r(x)$ is nonzero. Let $f_p^{(r)}$ be the number of $\overline{\mathbf{F}}_p$–valued points of the spectrum of the ring $\mathbf{Z}[T_r] \simeq \mathbf{Z}[x]/(h_r(x))$, then*

$$|\mathcal{E}(p,k)| \geq f_p^{(r)} \geq n_k - \nu_p(\delta_r). \tag{3.4}$$

Moreover if $f_p^{(r)} = n_k - \nu_p(\delta_r)$, then

$$|\mathcal{E}(p,k)| = f_p^{(r)} = n_k - \nu_p(\delta_r). \tag{3.5}$$

In this case p does not divide the index of $\mathbf{Z}[T_r]$ in its integral closure inside $\mathbf{Z}[T_r] \otimes \mathbf{Q} = \mathbf{T}_k^0 \otimes \mathbf{Q}$. In particular, p does not divide $[\mathbf{T}_k^0 : \mathbf{Z}[T_r]]$, we have $\nu_p(\delta_{\mathbf{T}_k^0}) = \nu_p(\delta_r)$, and the inclusion $\mathbf{Z}[T_r] \subset \mathbf{T}_k^0$ induces an isomorphism

$$\mathbf{F}_p[x]/(\bar{h}_r(x)) \simeq \mathbf{T}_k^0/p\mathbf{T}_k^0,$$

where $\bar{h}_r(x)$ denotes the reduction mod p of $h_r(x)$.

Notice that the integer $f_p^{(r)}$ is simply the degree of the largest square–free factor of the reduction mod p of $h_r(x)$.

As stated in the proposition, the subring $\mathbf{Z}[T_r] \subset \mathrm{End}_{\mathbf{C}}(\mathrm{M}_k^0)$ is isomorphic to $\mathbf{Z}[x]/(h_r(x))$ thanks to the assumption $\delta_r \neq 0$.

Definition. If the characteristic polynomial $h_r(x)$ of T_r acting on M_k^0 has nonzero discriminant and satisfies the numerical condition

$$f_p^{(r)} = n_k - \nu_p(\delta_r)$$

appearing in the second part of the proposition, then we will say that the Hecke operator T_r, acting on M_k^0, is p–good.

Of course the proposition can only be useful if one disposes of a Hecke operator T_r so that $\delta_r \neq 0$, which amounts to the requirement that the eigenvalues of T_r acting on M_k^0 be pairwise distinct. This condition is perhaps not too restrictive since in all known cases $h_r(x)$ is even *irreducible*, when $r > 1$.

Consider all pairs (p,k), where p is a prime number ≤ 2593, and k is an even integer $\leq p+1$ so that M_k^0 is nonzero. For each such pair, we looked for the least integer r, with $1 < r < 13$, such that T_r acting on M_k^0 is a p–good Hecke operator. In the table below we describe for how many pairs (p,k) a given r in the above range had such property.

r	2	3	5	6	7	10	11	12
	222039	256	36	5	13	2	4	2

TABLE 1. Number of pairs (p,k) such that T_r is p–good on M_k^0

Out of the 222370 pairs (p,k) considered, in only 13 cases there is no integer $r < 13$ (and there seems to be no integer at all) so that T_r acting on M_k^0 is p–good. It is the ease of finding p–good Hecke operators which makes Proposition 3.2 efficient for computing the difference $n_k - |\mathcal{E}(p,k)|$.

The 13 pairs (p,k) for which we are unable to find a p–good Hecke operator acting on M_k^0 are: $(491,246)$, $(563,282)$, $(751,376)$, $(1399,700)$, $(1423,712)$, $(1567,784)$, $(1747,874)$, $(1823,912)$, $(1879,940)$, $(1931,916)$, $(2083,1044)$, $(2243,1122)$, $(2347,1174)$. All these pairs are of the form $(p,(p+1)/2)$, and the space $\mathrm{M}^0_{(p+1)/2}$ gives rise to a set of mod p systems of eigenvalues whose associated representations are of dihedral type. We have a good understanding of dihedral systems, and in subsection 3.4 we explain how we computed $|\mathcal{E}(p,k)|$ in these cases. As it turns out, in all these cases we have $|\mathcal{E}(p,k)| = n_k$.

Overall we found that $n_k - |\mathcal{E}(p,k)|$ is always < 3, and the number of times the values $0, 1$ and 2 are attained are described by the next table, which gives an idea of how rare congruences are in this setting.

t	0	1	2
$\lvert\{(p,k) \mid n_k - \mathcal{E}(p,k) = t\}\rvert$	222171	198	1

TABLE 2. Number of pairs (p,k) such that $n_k - |\mathcal{E}(p,k)| = t$

Remark. Let $\tilde{\mathbf{T}}_k^0$ be the integral closure of the Hecke ring $\mathbf{T}_k^0$ in $\mathbf{T}_k^0 \otimes \mathbf{Q}$. For all the pairs (p,k) considered, p does not divide the index of $\mathbf{T}_k^0$ in $\tilde{\mathbf{T}}_k^0$. This follows from Proposition 3.2 whenever there exists a p–good Hecke operator T_r acting on M_k^0, and it follows from the equality $|\mathcal{E}(p,k)| = n_k$ in the remaining 13 cases. The conclusion is that, if $k \leq p+1$ and $p \leq 2593$, we have $\mathrm{Hom}_{\mathrm{rings}}(\mathbf{T}_k^0, \overline{\mathbf{F}}_p) = \mathrm{Hom}_{\mathrm{rings}}(\tilde{\mathbf{T}}_k^0, \overline{\mathbf{F}}_p)$, and there is no example of a mod p congruence between two distinct eigensystems arising from M_k^0 caused by the fact that the order $\mathbf{T}_k^0$ is not maximal at p. In other words, all the mod p congruences between distinct characteristic zero

Hecke eigensystems arising from M_k^0 that we had found can be explained in terms of ramification properties above p of the components of $\mathbf{T}_k^0 \otimes \mathbf{Q}$.

3.3. An upper bound for $|\mathcal{E}^{p-\mathrm{tame}}(p,k)|$. The set $\mathcal{E}^{p-\mathrm{tame}}(p,k)$ is the disjoint union of $\mathcal{E}^{p-\mathrm{split}}(p,k)$ and $\mathcal{E}^{p-\mathrm{irr}}(p,k)$, and we will bound these two sets separately using an analogous method. In order to bound the size of $\mathcal{E}^{p-\mathrm{split}}(p,k)$ (resp. $\mathcal{E}^{p-\mathrm{irr}}(p,k)$) we need to estimate how often there exists a system of eigenvalues Φ arising from $\mathrm{M}_k^0(\overline{\mathbf{F}}_p)$ so that the eigensystem $\Phi^{(1-k)}$ (resp. $\Phi^{(2-k)}$) arises from $\mathrm{M}_{p+1-k}^0(\overline{\mathbf{F}}_p)$ (resp. $\mathrm{M}_{p+3-k}^0(\overline{\mathbf{F}}_p)$) (cf. Theorem 2.3).

Let $h(x)$ and $j(x)$ be monic polynomials in $\mathbf{Z}[x]$ and let p be any prime number. Consider the greatest common divisor $d_p(x) \in \mathbf{F}_p[x]$ of the reduction mod p of $h(x)$ and $j(x)$.

Definition. The *linking number at p* of $h(x)$ and $j(x)$ is the degree of $d_p(x)$, it is denoted by $e_p(h,j)$.

The integer $e_p(h,j)$ is a measure of the congruences mod p between the roots of $h(x)$ and $j(x)$. It is zero if and only if the reduction mod p of $h(x)$ and $j(x)$ have no common roots in $\overline{\mathbf{F}}_p$.

Proposition 3.3. *Let ℓ be any prime $\neq p$, $h(x) \in \mathbf{Z}[x]$ the characteristic polynomial of T_ℓ acting on M_k^0, and $j(x) \in \mathbf{Z}[x]$ the characteristic polynomial of $\ell^{k-1}T_\ell$ acting on M_{p+1-k}^0. Then*

$$|\mathcal{E}^{p-\mathrm{split}}(p,k)| \leq e_p(h,j).$$

Proof. Let $\Phi = (a_q)_{q\neq p}$ be a system of eigenvalues arising from $\mathrm{M}_k^0(\overline{\mathbf{F}}_p)$ so that ρ_Φ is irreducible. By the tameness criterion established by Gross (cf. Thm. 2.3 ii)), the restriction of ρ_Φ to a decomposition group at p is decomposable if and only if there exists a system of mod p eigenvalues $(b_q)_{q\neq p}$ arising from $\mathrm{M}_{p+1-k}^0(\overline{\mathbf{F}}_p)$ so that

$$a_q = q^{k-1}b_q,$$

for all primes $q \neq p$. In particular, setting $q = \ell$, we see that

$$|\mathcal{E}^{p-\mathrm{split}}(p,k)| \leq e_p(h,j),$$

where $e_p(h,j)$ is the linking number at p of the polynomials $h(x)$ and $j(x)$. The proposition follows. □

Similarly we have (cf. Thm. 2.3 i)):

Proposition 3.4. *Let ℓ be any prime $\neq p$, $h(x) \in \mathbf{Z}[x]$ the characteristic polynomial of T_ℓ acting on M_k^0, and $j(x) \in \mathbf{Z}[x]$ the characteristic polynomial of $\ell^{k-2}T_\ell$ acting on M_{p+3-k}^0. Then*

$$|\mathcal{E}^{p-\mathrm{irr}}(p,k)| \leq e_p(h,j).$$

For any given prime $\ell \neq p$, the two propositions provide upper bounds for $|\mathcal{E}^{p-\mathrm{split}}(p,k)|$ and $|\mathcal{E}^{p-\mathrm{irr}}(p,k)|$. In both cases we kept the best upper bound obtained for $\ell = 2$ and 3. In the special case where $k = (p+1)/2$ (resp. $k = (p+3)/2$), in order to bound $|\mathcal{E}^{p-\mathrm{split}}(p,k)|$ (resp. $|\mathcal{E}^{p-\mathrm{irr}}(p,k)|$) we considered the Hecke operator T_{ℓ_0}, where ℓ_0 is smallest prime $\ell \neq p$ that is not a quadratic residue mod p, for otherwise the characteristic polynomials of T_ℓ and $\ell^{k-1}T_\ell$ (resp. $\ell^{k-2}T_\ell$) acting on M_k^0 would have the same mod p reduction and the resulting upper bound would be $\dim_{\mathbf{C}}(\mathrm{M}_k^0)$, the worst possible.

Remark. The upper bounds for $|\mathcal{E}^{p-\mathrm{split}}(p,k)|$ and $|\mathcal{E}^{p-\mathrm{irr}}(p,k)|$ obtained with the methods of Propositions 3.3 and 3.4 turned out to be reasonably small. We find for example that $|\mathcal{E}^{p-\mathrm{split}}(p,k)|$ is zero for 221984 pairs (p,k) out of the total 222370 analyzed, and that $|\mathcal{E}^{p-\mathrm{irr}}(p,k)|$ is zero in 222143 cases. In the third and fourth column of the table of section 6 one can find the translation of this data in terms of an upper bound on the number of mod p Galois representations of $\mathbf{Q}$ (up to twisting by the mod p cyclotomic character), that are tamely ramified.

If h is the class number of $\mathbf{Q}(\sqrt{-p})$, then for $p \equiv 3 \bmod 4$ and $k = (p+1)/2$ it can be shown that the set $\mathcal{E}^{p-\mathrm{split}}(p,k)$ contains precisely $(h-1)/2$ eigensystems Φ so that $\Phi = \Phi^{(p-1)/2}$. These are the eigensystems whose associated representations are of dihedral type (cf. §3.4), in this case we have the inequality $\mathcal{E}^{p-\mathrm{split}}(p,(p+1)/2) \geq (h-1)/2$.

Summarizing, we observe that if p is a prime for which we find that $\mathcal{E}^{p-\mathrm{Irr}}(p,k)$ is empty for all $k \leq p+1$, and that the union of the sets $\mathcal{E}^{p-\mathrm{split}}(p,k)$ for $k \leq p+1$ consists of only dihedral eigensystems (necessarily all appearing in weight $k = (p+1)/2$), then our method leads to the exact value of $R(p)$, provided that we compute h. This happens for 201 primes, in the table of section 6 the corresponding values $L(p)$ appear starred.

3.4. The dihedral case. Let Φ be a system of mod p eigenvalues arising from $\mathrm{M}_k^0(\overline{\mathbf{F}}_p)$ so that ρ_Φ is of *dihedral type*, meaning that the projective image G of ρ_Φ in $\mathrm{PGL}_2(\overline{\mathbf{F}}_p)$ is isomorphic to a dihedral group $C_n \rtimes \mathbf{Z}/2\mathbf{Z}$, where C_n is a cyclic group of order $n \geq 2$ and the nontrivial element of $\mathbf{Z}/2\mathbf{Z}$ acts on C_n by inversion. Since ρ_Φ is, by definition, semi–simple, it follows that any representation ρ_Φ of dihedral type acts irreducibly.

Representations of dihedral type fit in the class of "small–image" representations and are the easiest to understand and classify. It can be shown that

Proposition 3.5. *Let Φ be an eigensystem arising from $\mathrm{M}_k^0(\overline{\mathbf{F}}_p)$, with $2 \leq k \leq p+1$. The representation ρ_Φ is of dihedral type if and only if $\Phi = \Phi^{(p-1)/2}$. In this case we have*

i) ρ_Φ is tamely ramified at p;

ii) $p \equiv 3 \ mod\ 4$, $k = (p+1)/2$;

iii) the local representation $(\rho_\Phi)_p$ *is described by the sum of the trivial character and the quadratic character* $\chi_p^{(p-1)/2}$, *where* χ_p *denotes the mod* p *cyclotomic character of* $G_p = G(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$;

iv) the image of ρ_Φ *is isomorphic to* $C_n \rtimes \mathbf{Z}/2\mathbf{Z}$, *with* n *odd;*

v) $\rho_\Phi = \mathrm{Ind}_K^Q(\Psi)$, *where* $K = \mathbf{Q}(\sqrt{-p})$, *and* $\Psi : G_K \to \overline{\mathbf{F}}_p^*$ *is a continuous, everywhere unramified character.*

Furthermore, there are precisely $(h-1)/2$ *distinct isomorphism classes of such* ρ_Φ, *where* h *is the class number of the imaginary quadratic field* $\mathbf{Q}(\sqrt{-p})$.

The last statement of the proposition is essentially a modularity result for dihedral representations. This case of Serre's Conjecture was known much earlier thanks to the work of Hecke (cf. [18]). For a discussion on dihedral representations the reader might consider also [17].

Remark. For a prime $p \equiv 3$ mod 4, a consequence of the proposition is that if ℓ is a prime that is not a quadratic residue mod p, then the mod p reduction $\bar{h}_\ell(x) \in \mathbf{F}_p[x]$ of the characteristic polynomial of T_ℓ acting on $\mathrm{M}_k^0(\overline{\mathbf{F}}_p)$ is divisible by $x^{(h-1)/2}$. Using this simple fact we succeeded in computing the value of $|\mathcal{E}(p,k)|$ in the few cases where we were not able to apply the criterion of Proposition 3.2.

4. Discriminants of $S_\mathbf{Q}$–rings

In the next two sections we describe the theoretical basis of our computations by working in an axiomatic setting. In this section we introduce a special class of rings generalizing orders of number fields and recall the definition and basic properties of their discriminant.

Definition. A ring R, commutative with identity, is called a *finite* $S_\mathbf{Q}$*–ring* if the following conditions are satisfied:

i) R is finite and free as a $\mathbf{Z}$–module;

ii) $R \otimes \mathbf{Q}$ is isomorphic to a product of fields.

The *rank* of R is its rank as a $\mathbf{Z}$–module.

Condition ii) can be replaced by

ii)' R is reduced;

without affecting the notion just introduced. These rings derive their name from the fact that they become semi–simple after tensoring with $\mathbf{Q}$. Our motivation for considering them is that the Hecke ring $\mathbf{T}_k^0$ is of this type.

It is clear at once that if R is a finite $S_\mathbf{Q}$–ring, and $R' \subset R$ is a subring of finite index, then R' is itself a finite $S_\mathbf{Q}$–ring of the same rank as R. Furthermore, the product of finitely many finite $S_\mathbf{Q}$–rings is also a finite $S_\mathbf{Q}$–ring. If $h(x) \in \mathbf{Z}[x]$ is a monic polynomial, then $R_h = \mathbf{Z}[x]/(h(x))$ is a

finite $S_{\mathbf{Q}}$–ring if and only if it is reduced, i.e., if and only if $h(x)$ is square free.

Let R be any finite $S_{\mathbf{Q}}$–ring of rank n, and regard it as a subring of $R \otimes \mathbf{Q}$ via the injection $a \to a \otimes 1$. The Artin ring $R \otimes \mathbf{Q}$ decomposes as the product of finitely many local Artin rings

$$R \otimes \mathbf{Q} \simeq \prod_{1 \le i \le r} K_i,$$

and the factors of the decomposition are in correspondence with its prime ideals. By assumption, every K_i is a field, necessarily finite over $\mathbf{Q}$; we have

$$n = \sum_{1 \le i \le r} [K_i : \mathbf{Q}].$$

The ring extension $\mathbf{Z} \subset R$ is finite and therefore integral. It follows that the integral closure $\tilde{R}$ of R in $R \otimes \mathbf{Q}$ coincides with that of $\mathbf{Z}$. Therefore, if R_i denotes the ring of integers of K_i, we see that

$$\tilde{R} = \prod_{1 \le i \le r} R_i.$$

Moreover R has finite index in $\tilde{R}$, since the ranks of both rings are equal to $\dim_{\mathbf{Q}}(R \otimes \mathbf{Q})$. We have shown:

Proposition 4.1. *Any finite $S_{\mathbf{Q}}$–ring R is isomorphic to a finite index subring of the product of the rings of integers R_i of finitely many number fields K_i.*

The *discriminant* δ_R of a finite $S_{\mathbf{Q}}$–ring R is defined to be the determinant of the bilinear form

$$R \times R \ni (x, y) \longrightarrow \mathrm{tr}(xy) \in \mathbf{Z},$$

where, for $a \in R$, $\mathrm{tr}(a)$ denotes the trace of the $\mathbf{Q}$–linear map

$$l_a : R \otimes \mathbf{Q} \longrightarrow R \otimes \mathbf{Q}$$

given by multiplication by $a \otimes 1$. It is easy to show that

$$\mathrm{tr}(a) = \sum_{\sigma} \sigma(a), \tag{4.1}$$

where the sum ranges over all the ring homomorphisms $\sigma : R \to \overline{\mathbf{Q}}$.

If R is the ring of integers of a number field K, then δ_R coincides with the discriminant δ_K of K.

The discriminant is multiplicative on any finite product of finite $S_{\mathbf{Q}}$–rings, and if $R' \subset R$ is a subring of finite index d, then $\delta_{R'} = \delta_R d^2$. In particular $\delta_R \neq 0$ for any finite $S_{\mathbf{Q}}$–ring R, since $\delta_K \neq 0$ for any number field K. If $h(x) \in \mathbf{Z}[x]$ is a monic, square free polynomial of discriminant δ_h, then $\delta_{R_h} = \delta_h$ (cf. [13], Chp. 2 Thm. 8).

5. Discriminants and $\overline{\mathbf{F}}_p$–valued points of $\mathrm{Spec}(R)$

The goal of this section is to prove Theorem 5.1 which, for a finite $S_{\mathbf{Q}}$–ring R, gives a lower bound for the number of $\overline{\mathbf{F}}_p$–valued points of $\mathrm{Spec}(R)$, in terms of the p–adic valuation of the discriminant of R. We also obtain a criterion (Proposition 5.1) which gives a sufficient condition for the index of a monogenic subring $\mathbf{Z}[T] \subset R$ to be prime to p.

For a prime number p, let ν_p denote the additive p–adic valuation of $\mathbf{Q}_p$, normalized so that $\nu_p(p) = 1$.

Lemma 5.1. *Let R be the ring of integers of a number field K of degree n over $\mathbf{Q}$ and of discriminant δ_K. If p is any prime, let f_p be the number of $\overline{\mathbf{F}}_p$–valued points of* $\mathrm{Spec}(R)$*. Then*

$$f_p \geq n - \nu_p(\delta_K).$$

Moreover, equality holds if and only if p is tamely ramified in R.

Proof. For a prime $\mathfrak{p}$ of K above p, let $f_{\mathfrak{p}}$ and $e_{\mathfrak{p}}$ denote, respectively, the inertial degree and ramification index associated to $\mathfrak{p}$. There is the well–known formula (cf. [15], I §5, Prop. 10)

$$\sum_{\mathfrak{p}} e_{\mathfrak{p}} f_{\mathfrak{p}} = n \tag{5.1}$$

where the sum ranges over all the primes of R above p.

Let $K_{\mathfrak{p}}$ be the completion at $\mathfrak{p}$ of K and $\mathfrak{p}^{r_{\mathfrak{p}}}$ be the different of the local extension $K_{\mathfrak{p}}/\mathbf{Q}_p$. We know that

$$r_{\mathfrak{p}} \geq e_{\mathfrak{p}} - 1, \tag{5.2}$$

and equality holds if and only if $\mathfrak{p}$ is tamely ramified (Serre, loc. cit. III, §6). The p–part of the discriminant δ_K is the product of the norms of the fractional ideals $\mathfrak{p}^{r_{\mathfrak{p}}}$ of K, as $\mathfrak{p}$ ranges among the prime ideals of R above p (Serre, loc. cit. III, §5). Therefore we have

$$\nu_p(\delta_K) = \sum_{\mathfrak{p}} f_{\mathfrak{p}} r_{\mathfrak{p}}.$$

Taking into account formula 5.1 and the inequality 5.2, we have

$$\sum_{\mathfrak{p}} f_{\mathfrak{p}} r_{\mathfrak{p}} \geq \sum_{\mathfrak{p}} f_{\mathfrak{p}}(e_{\mathfrak{p}} - 1) = n - \sum_{\mathfrak{p}} f_{\mathfrak{p}}.$$

Moreover, equality holds if and only if every $\mathfrak{p}$ is tamely ramified above p, that is if and only if p is tamely ramified in K. Observing that $\sum_{\mathfrak{p}} f_{\mathfrak{p}} = f_p$ concludes the proof of the lemma. □

From the proof of Lemma 5.1 we deduce two Corollaries:

Corollary 5.1. *If $\nu_p(\delta_K) \leq p - 1$ then p is tamely ramified in R. In particular $f_p = n - \nu_p(\delta_K)$.*

Proof. Assume that p is not tamely ramified in K, then there exists a prime $\mathfrak{p}_0$ of R above p so that $p|e_{\mathfrak{p}_0}$ and, in the notation used in the proof of Lemma 5.1, $r_{\mathfrak{p}_0} > e_{\mathfrak{p}_0} - 1$. In particular

$$r_{\mathfrak{p}_0} > e_{\mathfrak{p}_0} - 1 \geq p - 1.$$

By the proof of Lemma 5.1, we obtain

$$\nu_p(\delta_K) = \sum_{\mathfrak{p}} f_{\mathfrak{p}} r_{\mathfrak{p}} > p - 1,$$

which completes the proof of the corollary. □

Corollary 5.2. *If $\nu_p(\delta_K) = 1$ then there exists exactly one prime $\mathfrak{p}_0$ of R that lies above p and that is ramified. We have $e_{\mathfrak{p}_0} = 2$, $f_{\mathfrak{p}_0} = 1$, and* $\mathrm{Spec}(R)$ *has exactly $n - 1$ distinct $\overline{\mathbf{F}}_p$–valued points.*

Proof. By assumption $\nu_p(\delta_K) = 1 \leq p - 1$, therefore Corollary 5.1 ensures that p is tamely ramified in R. Applying Lemma 5.1 we obtain that the number f_p of distinct $\overline{\mathbf{F}}_p$–valued points of $\mathrm{Spec}(R)$ is

$$f_p = n - \nu_p(\delta_K) = n - 1,$$

and the last part of the corollary follows. To see the first part, observe that f_p is equal to the sum $\sum f_{\mathfrak{p}}$ of the inertial degrees of the primes of R of residual characteristic p. But since $f_p = n - 1$, we easily see that formula 5.1 forces the existence of exactly one ramified prime above p, say $\mathfrak{p}_0$, and for which, moreover, we must have $e_{\mathfrak{p}_0} = 2$ and $f_{\mathfrak{p}_0} = 1$. □

In order to prove Theorem 5.1 we need the following lemma:

Lemma 5.2. *Let $R' \subset R$ be an extension of finite $S_{\mathbf{Q}}$–rings so that R' has finite index d in R. Let f_p and f'_p be the numbers of $\overline{\mathbf{F}}_p$–valued points of, respectively,* $\mathrm{Spec}(R)$ *and* $\mathrm{Spec}(R')$*. Then*

$$f_p \geq f'_p \geq f_p - \nu_p(d).$$

Proof. The extension $R' \subset R$ is finite, therefore integral, and any $\overline{\mathbf{F}}_p$–valued point of $\mathrm{Spec}(R')$ can be lifted to one of $\mathrm{Spec}(R)$ (cf. [1] Theorem 5.16), and the first inequality $f_p \geq f'_p$ readily follows.

To see the other inequality, note that the inclusion $R' \subset R$ induces an injective ring homorphism

$$\iota : R'/I \hookrightarrow R/pR,$$

where $I = pR \cap R'$ is the ideal of R' given by the contraction of $(p) \subset R$, and R'/I may be identified with an $\mathbf{F}_p$–subalgebra of R/pR.

The cokernel of ι is an abelian group isomorphic to $(R/R')/p(R/R')$, we have

$$|(R/pR)/(R'/I)| = |(R/R')/p(R/R')| \leq p^{\nu_p(d)}.$$

If n (resp. n') is the dimension of R/pR (resp. R'/I) over $\mathbf{F}_p$, then the previous inequality implies

$$n - n' \leq \nu_p(d).$$

Let $\sqrt{0}$ (resp. $\sqrt{0}'$) be the nilradical ideal of R/pR (resp. R'/I), and let $(R/pR)_{\mathrm{red}}$ (resp. $(R'/I)_{\mathrm{red}}$) be the reduced ring associated to R/pR (resp. R'/I). We have the following exact sequences of $\mathbf{F}_p$–vector spaces:

$$0 \longrightarrow \sqrt{0} \longrightarrow R/p \longrightarrow \big(R/pR\big)_{\mathrm{red}} \longrightarrow 0,$$

$$0 \longrightarrow \sqrt{0}' \longrightarrow R'/I \longrightarrow \big(R'/I\big)_{\mathrm{red}} \longrightarrow 0.$$

Now, the injection $R'/I \hookrightarrow R/p$ induces the inclusions

$$\sqrt{0}' \subset \sqrt{0} \text{ and } \big(R'/I\big)_{\mathrm{red}} \subset \big(R/pR\big)_{\mathrm{red}}.$$

Therefore there is a natural morphism between the exact sequences above, from the lower to the upper one, described by three inclusions. If r (resp. r') is the dimension of $\sqrt{0}$ (resp. $\sqrt{0}'$), then we have

$$f'_p + r' - n' = f_p + r - n = 0,$$

since $r' \leq r$, we obtain

$$f'_p = f_p - (n - n') + (r - r') \geq f_p - \nu_p(d),$$

and this completes the proof of the lemma. □

Lemma 5.1 generalizes as follows:

Theorem 5.1. *Let R be a finite $S_{\mathbf{Q}}$–ring of rank n. If p is any prime number, let f_p denote the number of $\overline{\mathbf{F}}_p$–valued points of* $\mathrm{Spec}(R)$. *Then*

$$f_p \geq n - \nu_p(\delta_R).$$

Moreover, equality holds if and only if the index of R in its integral closure $\tilde{R}$ in $R \otimes \mathbf{Q}$ is prime to p and p is tamely ramified in each component of $R \otimes \mathbf{Q}$.

Proof. By Lemma 5.1, the inequality expressed by the theorem is satisfied when R is the ring of integers of a number field K. Note that the integers f_p and $\nu_p(\delta_R)$, viewed as functions of R, are additive with respect to finite product of $S_{\mathbf{Q}}$–rings. Therefore the inequality

$$f_p \geq n - \nu_p(\delta_R)$$

holds for any finite $S_{\mathbf{Q}}$–ring R that is isomorphic to a finite product of rings of integers R_i of number fields K_i, i.e. the inequality of the theorem is proved for any finite $S_{\mathbf{Q}}$–ring R that is integrally closed in $R \otimes \mathbf{Q}$. In this case the second part of the theorem follows immediately from Lemma 5.1.

Let now R be any finite $S_{\mathbf{Q}}$–ring, let $\tilde{R} \subset R \otimes \mathbf{Q}$ be its integral closure, and let d be the (finite) index $[\tilde{R} : R]$. If $\tilde{f}_p$ denote the number of $\overline{\mathbf{F}}_p$–valued points of $\mathrm{Spec}(\tilde{R})$, then Lemma 5.2 applied to the extension $R \subset \tilde{R}$ says that

$$f_p \geq \tilde{f}_p - \nu_p(d).$$

We have seen that the theorem holds for $\tilde{R}$, therefore

$$f_p \geq n - \nu_p(\delta_{\tilde{R}}) - \nu_p(d).$$

Since $\delta_R = \delta_{\tilde{R}} d^2$ we have

$$-\nu_p(\delta_{\tilde{R}}) - \nu_p(d) \geq -\nu_p(\delta_R), \tag{5.3}$$

and therefore

$$f_p \geq n - \nu_p(\delta_R),$$

completing the proof of the first part of the theorem. Now if p divided d, then inequality (5.3) would certainly be strict and, consequently, f_p would be strictly greater than $n - \nu_p(\delta_R)$. □

The following proposition is a consequence of Theorem 5.1 and Lemma 5.2 and gives a criterion for counting the number of $\overline{\mathbf{F}}_p$–valued points of $\mathrm{Spec}(R)$ in terms of numerical data encoded in the characteristic polynomial of an element $T \in R$ that generates a finite index subring $\mathbf{Z}[T] \subset R$. It will be useful in our computations when R is a Hecke ring $\mathbf{T}_k^0$ and T is an Hecke operator T_ℓ.

Proposition 5.1. *Let R be a finite $S_{\mathbf{Q}}$–ring of rank n, $T \in R$ any element, and $h(x) \in \mathbf{Z}[x]$ its characteristic polynomial. Assume that the discriminant δ_h of $h(x)$ is nonzero. Let f_p be the number of $\overline{\mathbf{F}}_p$–valued points of* $\mathrm{Spec}(R)$ *and $f_p^{(h)}$ that of the spectrum of $\mathbf{Z}[T] = \mathbf{Z}[x]/(h(x))$, then*

$$f_p \geq f_p^{(h)} \geq n - \nu_p(\delta_h).$$

Moreover if $f_p^{(h)} = n - \nu_p(\delta_h)$, then

$$f_p = f_p^{(h)} = n - \nu_p(\delta_h). \tag{5.4}$$

In this case p does not divide the index $\mathbf{Z}[T]$ in its integral closure in $\mathbf{Z}[T] \otimes \mathbf{Q} = R \otimes \mathbf{Q}$. In particular, p does not divide the index $[R : \mathbf{Z}[T]]$, we have $\nu_p(\delta_R) = \nu_p(\delta_h)$, and the inclusion $\mathbf{Z}[T] \subset R$ induces an isomorphism

$$\mathbf{Z}[T]/p\mathbf{Z}[T] \simeq R/pR.$$

The characteristic polynomial $h(x)$ of $T \in R$ alluded to in the proposition is the monic characteristic polynomial of the endomorphism of the $\mathbf{Q}$–vector space $R \otimes \mathbf{Q}$ given by multiplication by $T \otimes 1$.

Notice that $f_p^{(h)}$ is simply the number of distinct roots in $\overline{\mathbf{F}}_p$ of the reduction mod p of $h(x)$, and n is the degree of $h(x)$. Thus the equality $f_p^{(h)} = n - \nu_p(\delta_h)$ is a numerical condition on $h(x)$.

Proof. The ring R is a finite $S_{\mathbf{Q}}$–ring and has no nilpotent elements. It follows that the endomorphism of $R \otimes \mathbf{Q}$ given by multiplication by $T \otimes 1$ is semi–simple, meaning that its minimal polynomial is square free. Moreover, by assumption, the characteristic polynomial $h(x)$ of T is square free and we conclude that $h(x)$ is equal to the minimal polynomial of T. It follows that the subring $\mathbf{Z}[T]$ has rank n as an abelian group, hence the index $[R : \mathbf{Z}[T]]$ is finite, say equal to d.

Lemma 5.2 says that

$$f_p \geq f_p^{(h)} \geq f_p - \nu_p(d),$$

from which the first part of the proposition follows. Theorem 5.1 implies that

$$f_p \geq n - \nu_p(\delta_R),$$

and, since $\delta_h = \delta_r d^2$, putting together the two inequalities yields

$$f_p \geq f_p^{(h)} \geq f_p - \nu_p(d) \geq n - \nu_p(\delta_R) - \nu_p(d) \geq n - \nu_p(\delta_h). \tag{5.5}$$

Notice that the last inequality to the right is *strict* if p divides d.

Now if $f_p^{(h)} = n - \nu_p(\delta_h)$, then the last three inequalities of (5.5) are forced to be equalities. This immediately implies that $\nu_p(d) = 0$ and $f_p = f_p^{(h)}$, and we see that (5.4) of the proposition holds.

To complete the proof of the proposition we are only left with showing that p does not divide the index of $\mathbf{Z}[T]$ in its integral closure, provided that the equality $f_p^{(h)} = n - \nu_p(\delta_h)$ holds. We had just shown that p does not divide the index $[R : \mathbf{Z}[T]]$. Replacing R by its integral closure $\tilde{R}$ and reasoning as above we easily see that p does not divide $[\tilde{R} : \mathbf{Z}[T]]$, and the proposition follows. □

Remark. If there exists $T \in R$ so that $\nu_p(\delta_h) \leq 1$, then one knows that the equality $f_p^{(h)} = n - \nu_p(\delta_h)$ is automatically satisfied. This is clear if $\nu_p(\delta_h) = 0$, since in that case the reduction mod p of $h(x)$ is square free, and therefore $f_p^{(h)} = n$. In the case where $\nu_p(\delta_h) = 1$, we have that $h(x)$ has multiple roots when reduced mod p, therefore $n > f_p^{(h)}$. On the other hand, by Theorem 5.1, we have $f_p^{(h)} \geq n - \nu_p(\delta_h) = n - 1$, therefore $f_p^{(h)} = n - 1$ and the equality $f_p^{(h)} = n - \nu_p(\delta_h)$ holds. In this last case, namely when $\nu_p(\delta_R) = 1$, a complete description of the ramification of the components of $R \otimes \mathbf{Q}$ can be given: all of them but one are unramified above p, moreover the ramification above p in the ramified component is that described in Corollary 5.2.

6. Table of results

In this last section we present and explain the table containing the results of our computations. Recall that formula (3.3) in section 3 says

$$R(p) = (p-1) \sum_{2 \leq k \leq p+1} \left[|\mathcal{E}(p,k)| - |\mathcal{E}^{\mathrm{Eis}}(p,k)| - \frac{1}{2} |\mathcal{E}^{p-\mathrm{tame}}(p,k)| \right],$$

where $\mathcal{E}(p,k)$, $\mathcal{E}^{\mathrm{Eis}}(p,k)$ and $\mathcal{E}^{p-\mathrm{tame}}(p,k)$ are, respectively, the set of systems of eigenvalues mod p arising from the Hecke module $\mathrm{M}_k^0(\overline{\mathbf{F}}_p)$; its subset given by those eigensystems Φ for which the associated mod p Galois representation ρ_Φ of $\mathbf{Q}$ is reducible; and the subset of the Φ such that ρ_Φ is irreducible and tamely ramified at p.

In subsections 3.1 and 3.2 we discussed how we computed the cardinalities of $\mathcal{E}(p,k)$ and $\mathcal{E}^{\mathrm{Eis}}(p,k)$, and in subsection 3.3 we explained how we obtained an upper bound for the size of $\mathcal{E}^{p-\mathrm{tame}}(p,k)$, which is the disjoint union of $\mathcal{E}^{p-\mathrm{split}}(p,k)$ and $\mathcal{E}^{p-\mathrm{irr}}(p,k)$ (cf. §3.3).

This of course results in providing a lower bound $L(p)$ of $R(p)$; furthermore the value of $L(p)$ is the actual value of $R(p)$ as soon as the estimate that we have for $|\mathcal{E}^{p-\mathrm{tame}}(p,k)|$ is in fact equal to its value for all $k \leq p+1$.

The columns of the table contain the following data:

(p): the list of primes $p \leq 2593$ for which there exists a space of cusp forms of weight k, with $k \leq p+1$, that is nonzero;

(r): the value $\sum_{2 \leq k \leq p+1} |\mathcal{E}^{\mathrm{Eis}}(p,k)|$, which gives the total number of systems of eigenvalues mod p corresponding to reducible representations, and arising from the spaces $\mathrm{M}_k^0(\overline{\mathbf{F}}_p)$, where $k \leq p+1$;

(u_a): one half of the difference between the upper bound obtained for the sum $\sum_{2 \leq k \leq p+1} |\mathcal{E}^{p-\mathrm{split}}(p,k)|$ and the number of dihedral representations;

(u_b): one half of the upper bound of the sum $\sum_{2 \leq k \leq p+1} |\mathcal{E}^{p-\mathrm{irr}}(p,k)|$;

(L): the value of the lower bound $L(p)$ of $R(p)$;

(Δ/p^2): the ratio between $\Delta(p) = U(p) - L(p)$ and p^2.

Observe that u_a gives an upper bound on the number of isomorphisms classes, up to twist by the mod p cyclotomic character, of Galois representations ρ of $\mathbf{Q}$ of the type considered, such that ρ is non–dihedral and the local representation ρ_p is decomposable. Similarly, u_b controls from above the number of Galois representations of $\mathbf{Q}$, up to twist, that are irreducible locally at p. Finally, observe that whenever for given prime p the corresponding values of u_a and u_b are zero, we can determine the exact value of $\sum_{2 \leq k \leq p+1} |\mathcal{E}^{p-\mathrm{tame}}(p,k)|$, this in fact coincides with the number of representations ρ of the type considered and that are dihedral (cf. §3.4). In this case $L(p)$ is the exact value of $R(p)$, and appears starred in the table.

p	r	u_a	u_b	L	Δ/p^2	p	r	u_a	u_b	L	Δ/p^2
11	0	0	0	10*	0.0000	211	0	0	0	185535*	0.0023
13	0	0	0	12*	0.0000	223	0	0	1	219225	0.0111
17	0	0	0	48*	0.0000	227	0	0	0	231424*	0.0131
19	0	0	0	72*	0.0000	229	0	2	1	237576	0.0130
23	0	0	0	143*	0.0207	233	1	0	0	250792*	0.0085
29	0	0	0	336*	0.0000	239	0	0	0	270725*	0.0145
31	0	0	0	405*	0.0156	241	0	1	0	277680	0.0123
37	1	0	0	720*	0.0262	251	0	0	0	314875*	0.0059
41	0	0	0	1080*	0.0000	257	1	0	3	337664	0.0155
43	0	0	0	1260*	0.0000	263	1	0	1	362084	0.0189
47	0	0	0	1656*	0.0208	269	0	1	1	388332	0.0111
53	0	0	0	2496*	0.0000	271	1	2	0	396495	0.0202
59	1	0	1	3393	0.0416	277	0	0	1	425040	0.0035
61	0	0	0	3900*	0.0000	281	0	0	0	444360*	0.0000
67	1	0	0	5148*	0.0294	283	1	1	2	452751	0.0158
71	0	0	0	6195*	0.0347	293	1	0	0	503408*	0.0136
73	0	0	0	6840*	0.0135	307	1	1	1	580023	0.0146
79	0	0	1	8736	0.0249	311	1	2	0	602485	0.0240
83	0	0	0	10373*	0.0059	313	0	0	1	616200	0.0031
89	0	0	0	12848*	0.0111	317	0	0	0	640532*	0.0031
97	0	0	0	16896*	0.0000	331	0	2	2	729135	0.0135
101	1	0	0	19100*	0.0098	337	0	0	0	771456*	0.0000
103	1	0	0	20196*	0.0192	347	1	1	0	842164	0.0086
107	0	1	1	22737	0.0231	349	0	0	0	857472*	0.0028
109	0	0	0	24300*	0.0000	353	2	0	2	886336	0.0141
113	0	0	0	27104*	0.0087	359	0	0	0	933127*	0.0124
127	0	0	0	38934*	0.0078	367	0	0	0	998448*	0.0054
131	1	0	1	42510	0.0303	373	0	0	1	1049040	0.0026
137	0	0	0	49368*	0.0000	379	2	1	1	1099791	0.0118
139	0	1	1	50991	0.0321	383	0	0	0	1135686*	0.0104
149	1	0	0	63788*	0.0066	389	1	0	0	1190772*	0.0076
151	0	1	1	66075	0.0230	397	0	1	0	1266804	0.0050
157	2	0	0	74256*	0.0316	401	1	0	0	1306000*	0.0049
163	0	0	0	83916*	0.0121	409	1	0	0	1386792*	0.0024
167	0	0	0	90387*	0.0148	419	0	0	1	1491006	0.0095
173	0	1	1	100620	0.0172	421	1	1	0	1513260	0.0047
179	0	1	0	111784	0.0166	431	0	1	0	1623250	0.0138
181	0	0	0	115920*	0.0054	433	1	1	0	1646352	0.0115
191	0	2	0	136040	0.0260	439	0	1	1	1716303	0.0124
193	0	1	1	140928	0.0103	443	0	0	0	1766232*	0.0022
197	0	0	0	150528*	0.0000	449	0	0	0	1839040*	0.0044
199	0	0	0	154836*	0.0099	457	0	0	0	1939824*	0.0043

p	r	u_a	u_b	L	Δ/p^2	p	r	u_a	u_b	L	Δ/p^2
461	1	0	0	1992260*	0.0021	739	0	0	0	8281836*	0.0027
463	1	0	1	2017323	0.0075	743	0	1	0	8414280	0.0094
467	2	0	0	2070205*	0.0096	751	1	2	0	8690625	0.0086
479	0	1	1	2233216	0.0187	757	1	0	0	8904924*	0.0026
487	0	0	0	2351025*	0.0051	761	1	0	1	9047800	0.0026
491	3	2	2	2406880	0.0182	769	0	0	1	9337344	0.0025
499	0	0	1	2530587	0.0049	773	1	1	0	9484792	0.0025
503	0	1	0	2590320	0.0138	787	0	0	0	10012854*	0.0012
509	0	0	0	2688336*	0.0000	797	1	0	0	10401332*	0.0012
521	0	0	0	2883400*	0.0038	809	2	0	0	10878912*	0.0037
523	1	0	0	2916414*	0.0057	811	1	0	1	10958895	0.0055
541	1	0	1	3230820	0.0036	821	1	0	0	11373400*	0.0024
547	2	0	0	3339609*	0.0063	823	0	0	0	11457036*	0.0024
557	1	0	0	3528376*	0.0035	827	1	0	0	11624711*	0.0042
563	0	1	0	3643446	0.0070	829	0	0	0	11712060*	0.0000
569	0	1	0	3763000	0.0035	839	1	0	1	12133402	0.0142
571	0	0	0	3803040*	0.0034	853	0	0	1	12762960	0.0011
577	1	1	1	3924288	0.0051	857	0	1	0	12943576	0.0023
587	2	0	0	4132765*	0.0076	859	0	0	0	13035165*	0.0017
593	1	0	0	4263584*	0.0016	863	0	0	0	13215322*	0.0069
599	0	1	1	4389918	0.0166	877	1	0	0	13874964*	0.0022
601	0	0	1	4438800	0.0033	881	1	0	0	14066800*	0.0022
607	1	0	0	4572876*	0.0065	883	0	0	1	14163597	0.0016
613	1	0	0	4712400*	0.0016	887	1	0	0	14352314*	0.0090
617	3	0	0	4804184*	0.0064	907	0	0	1	15355341	0.0016
619	1	2	0	4851300	0.0064	911	0	1	0	15553265	0.0104
631	2	0	0	5140170*	0.0079	919	0	1	0	15970905	0.0070
641	0	0	0	5393280*	0.0000	929	2	0	0	16504480*	0.0021
643	0	1	0	5443197	0.0023	937	0	0	0	16937856*	0.0000
647	3	0	1	5541065	0.0146	941	0	0	0	17156880*	0.0000
653	1	0	3	5701088	0.0061	947	0	0	0	17487756*	0.0010
659	1	0	0	5861135*	0.0053	953	1	0	0	17822392*	0.0020
661	0	0	0	5914260*	0.0060	967	0	2	0	18619167	0.0056
673	2	0	0	6245568*	0.0029	971	1	0	0	18853405*	0.0046
677	1	0	0	6357780*	0.0044	977	0	0	0	19210608*	0.0000
683	1	0	0	6529468*	0.0043	983	0	1	0	19558985	0.0096
691	2	0	0	6762000*	0.0057	991	0	1	0	20046510	0.0050
701	0	0	1	7063700	0.0014	997	0	0	0	20418996*	0.0000
709	0	0	0	7309392*	0.0014	1009	0	1	0	21164976	0.0029
719	0	0	1	7619057	0.0131	1013	0	0	0	21422016*	0.0000
727	1	0	0	7881456*	0.0054	1019	0	1	0	21800470	0.0058
733	0	1	0	8080548	0.0027	1021	0	0	0	21935100*	0.0000

p	r	u_a	u_b	L	Δ/p^2	p	r	u_a	u_b	L	Δ/p^2
1031	0	0	0	22580175*	0.0082	1319	1	0	0	47392644*	0.0098
1033	0	0	0	22720512*	0.0000	1321	0	1	1	47622960	0.0015
1039	0	0	0	23113665*	0.0062	1327	1	0	0	48273693*	0.0033
1049	0	0	1	23795888	0.0009	1361	0	0	0	52097520*	0.0000
1051	0	0	1	23931600	0.0019	1367	1	0	0	52778142*	0.0073
1061	1	0	2	24622740	0.0028	1373	0	1	2	53486048	0.0029
1063	0	0	1	24758937	0.0061	1381	1	0	2	54429960	0.0021
1069	0	0	1	25187712	0.0009	1399	0	1	0	56586147	0.0053
1087	0	0	1	26484282	0.0027	1409	1	0	0	57820928*	0.0007
1091	1	0	0	26776940*	0.0045	1423	0	1	0	59561892	0.0028
1093	0	2	0	26927628	0.0018	1427	0	0	1	60066685	0.0031
1097	0	2	0	27224640	0.0027	1429	1	1	0	60321576	0.0020
1103	0	0	0	27672873*	0.0049	1433	0	0	0	60835656*	0.0000
1109	0	0	0	28134336*	0.0000	1439	1	0	1	61588821	0.0079
1117	1	0	1	28747044	0.0017	1447	0	0	0	62631321*	0.0044
1123	0	0	1	29214636	0.0017	1451	0	0	0	63159100*	0.0020
1129	1	0	2	29684448	0.0035	1453	0	0	1	63423360	0.0006
1151	3	0	0	31449050*	0.0121	1459	0	0	0	64211049*	0.0023
1153	1	0	0	31627008*	0.0017	1471	0	0	0	65808225*	0.0044
1163	0	0	0	32459889*	0.0021	1481	0	0	1	67169800	0.0013
1171	0	0	0	33137325*	0.0012	1483	1	0	1	67440633	0.0023
1181	0	1	2	33992260	0.0042	1487	0	0	0	67980042*	0.0067
1187	0	0	3	34513786	0.0050	1489	0	0	1	68266464	0.0013
1193	1	0	0	35047184*	0.0008	1493	0	0	0	68822976*	0.0000
1201	1	1	0	35756400	0.0024	1499	1	0	0	69649510*	0.0039
1213	0	0	0	36846012*	0.0000	1511	0	1	0	71329380	0.0085
1217	3	0	0	37208384*	0.0032	1523	1	0	0	73062849*	0.0016
1223	0	0	0	37757967*	0.0069	1531	0	0	1	74219535	0.0029
1229	1	0	1	38325880	0.0016	1543	0	1	0	75979737	0.0042
1231	0	0	1	38506995	0.0060	1549	0	1	0	76879872	0.0006
1237	1	0	0	39081084*	0.0016	1553	0	0	3	77474288	0.0025
1249	0	0	1	40234272	0.0007	1559	1	0	0	78363505*	0.0086
1259	0	0	1	41206419	0.0043	1567	0	0	0	79594299*	0.0022
1277	0	1	1	43008856	0.0015	1571	0	0	0	80206590*	0.0025
1279	1	0	0	43205985*	0.0050	1579	0	0	1	81442158	0.0018
1283	1	0	0	43618127*	0.0027	1583	0	0	0	82056758*	0.0050
1289	0	0	0	44237648*	0.0007	1597	1	3	0	84262416	0.0031
1291	2	0	1	44437920	0.0046	1601	0	0	0	84905600*	0.0006
1297	2	0	0	45067104*	0.0015	1607	0	0	0	85857563*	0.0040
1301	1	0	0	45485700*	0.0023	1609	1	0	0	86185584*	0.0012
1303	0	1	0	45694341	0.0034	1613	1	0	0	86831992*	0.0012
1307	2	0	0	46118125*	0.0034	1619	1	0	1	87799961	0.0040

p	r	u_a	u_b	L	Δ/p^2	p	r	u_a	u_b	L	Δ/p^2
1621	1	0	0	88134480*	0.0006	1979	1	0	0	160561183*	0.0037
1627	0	0	1	89116995	0.0015	1987	1	1	0	162525303	0.0022
1637	1	0	1	90775096	0.0012	1993	1	0	0	164011320*	0.0005
1657	0	1	0	94151880	0.0006	1997	2	0	1	164995348	0.0025
1663	2	1	0	95171106	0.0042	1999	0	0	0	165487347*	0.0037
1667	0	0	0	95868304*	0.0017	2003	2	1	0	166490324	0.0024
1669	2	1	0	96213576	0.0017	2011	0	1	0	168501315	0.0012
1693	0	0	0	100438812*	0.0000	2017	1	0	0	170019360*	0.0004
1697	0	1	0	101152832	0.0005	2027	0	0	0	172561511*	0.0017
1699	0	0	0	101508987*	0.0014	2029	0	0	3	173069520	0.0024
1709	0	2	0	103315212	0.0017	2039	1	1	0	175628726	0.0068
1721	1	0	0	105513400*	0.0011	2053	1	0	2	179299656	0.0014
1723	0	0	1	105880614	0.0017	2063	0	1	1	181917888	0.0062
1733	2	0	2	107737328	0.0023	2069	0	0	0	183539136*	0.0000
1741	0	0	0	109245900*	0.0000	2081	0	0	0	186756960*	0.0000
1747	0	0	0	110376882*	0.0017	2083	0	2	0	187283187	0.0031
1753	1	0	0	111523560*	0.0005	2087	2	0	1	188356413	0.0055
1759	1	0	0	112662309*	0.0048	2089	0	0	1	188920152	0.0004
1777	1	0	0	116175264*	0.0011	2099	1	0	0	191642859*	0.0026
1783	0	1	0	117353610	0.0028	2111	1	0	2	194932350	0.0075
1787	1	0	2	118144793	0.0036	2113	0	0	0	195520512*	0.0000
1789	2	0	0	118546188*	0.0022	2129	0	0	0	200004336*	0.0000
1801	0	1	0	120958200	0.0005	2131	0	0	0	200560800*	0.0018
1811	3	0	1	122974115	0.0052	2137	1	0	1	202264248	0.0014
1823	0	1	0	125433768	0.0071	2141	0	1	0	203409140	0.0004
1831	1	0	0	127107225*	0.0035	2143	1	0	0	203971950*	0.0023
1847	3	0	0	130463281*	0.0073	2153	1	0	0	206854544*	0.0004
1861	0	0	0	133481040*	0.0005	2161	0	0	0	209174400*	0.0000
1867	0	0	0	134777448*	0.0010	2179	0	0	0	214449147*	0.0011
1871	1	0	0	135629230*	0.0064	2203	0	0	1	221626896	0.0009
1873	0	0	0	136086912*	0.0000	2207	0	1	0	222820339	0.0047
1877	1	1	1	136953628	0.0026	2213	1	2	1	224659568	0.0018
1879	1	1	0	137386029	0.0045	2221	0	0	0	227117100*	0.0000
1889	1	0	0	139610048*	0.0005	2237	0	1	1	232065496	0.0008
1901	1	1	0	142291000	0.0010	2239	1	1	0	232668075	0.0051
1907	0	1	0	143639972	0.0026	2243	0	2	2	233929159	0.0033
1913	0	1	1	145006080	0.0015	2251	0	0	1	236455875	0.0011
1931	0	2	3	149133030	0.0051	2267	1	0	1	241531807	0.0033
1933	2	0	0	149612148*	0.0010	2269	0	0	1	242186112	0.0004
1949	0	2	0	153366040	0.0010	2273	2	0	0	243467520*	0.0013
1951	1	0	0	153821850*	0.0056	2281	0	0	0	246055320*	0.0004
1973	0	1	2	159108848	0.0020	2287	0	0	0	247992138*	0.0030

p	r	u_a	u_b	L	Δ/p^2	p	r	u_a	u_b	L	Δ/p^2
2293	1	0	3	249958644	0.0017	2423	2	0	0	294987490*	0.0049
2297	0	0	0	251278832*	0.0004	2437	0	0	0	300163920*	0.0004
2309	2	0	0	255239412*	0.0012	2441	2	0	0	301642560*	0.0012
2311	0	1	0	255892560	0.0034	2447	0	4	0	303849458	0.0057
2333	0	0	0	263299124*	0.0004	2459	0	0	1	308367161	0.0026
2339	0	0	0	265331437*	0.0019	2467	0	0	1	311392917	0.0022
2341	0	0	0	266020560*	0.0004	2473	0	0	1	313684440	0.0004
2347	0	0	0	268075074*	0.0004	2477	0	0	0	315212132*	0.0004
2351	0	0	0	269416925*	0.0065	2503	1	0	0	325244988*	0.0023
2357	1	0	0	271521932*	0.0004	2521	0	0	0	332337600*	0.0000
2371	2	0	0	276387030*	0.0021	2531	0	0	1	336302780	0.0019
2377	1	0	0	278502840*	0.0004	2539	0	1	0	339506991	0.0017
2381	1	1	0	279911800	0.0008	2543	1	0	0	341104625*	0.0037
2383	2	0	1	280599600	0.0041	2549	0	1	0	343549388	0.0003
2389	1	0	0	282748752*	0.0004	2551	0	0	0	344336700*	0.0039
2393	0	1	0	284174384	0.0004	2557	1	1	0	346795524	0.0007
2399	0	0	1	286284031	0.0068	2579	1	0	1	355825872	0.0027
2411	1	0	1	290627925	0.0035	2591	2	0	0	360797360*	0.0065
2417	0	0	2	292819200	0.0012	2593	0	2	0	361672128	0.0007

TABLE 3. Table of results

References

[1] M. F. Atiyah, I.G. Macdonald, *Introduction to Commutative Algebra*. Addison-Wesley, 1969.

[2] A. Ash, G. Stevens, *Modular Forms in characteristic ℓ and special values of their L-functions*. Duke Math. J. **53** (1986), no.3, 849–868.

[3] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system. I. The user language*. J. Symbolic Comput. **24** (1997), 235–265.

[4] C. Citro, A. Ghitza, *Enumerating Galois representations in Sage*. Preprint available at http://arxiv.org/abs/1006.4084.

[5] B. Edixhoven, *The weight in Serre's conjecture on modular forms*. Invent. Math. **109** (1992), 563–594.

[6] B. Gross, *A tameness criterion for Galois representations associated to modular forms (mod p)*. Duke Math. J. **61** (1990), no. 2, 445–517.

[7] N. Jochnowitz, *A study of the local components of the Hecke Algebra mod l*. Trans. Amer. Math. Soc. **270** (1982), no.1, 253–267.

[8] N. Jochnowitz, *Congruences between systems of eigenvalues of modular forms*. Trans. Amer. Math. Soc. **270** (1982), no.1, 269–285.

[9] N. Katz, *p-adic properties of modular schemes and modular forms*. Modular Functions of One Variable III, Lecture Notes in Math. **350**, 69–190. Springer–Verlag, 1973.

[10] C. Khare, *Modularity of Galois representations and motives with good reduction properties*. J. Ramanujan Math. Soc. **22** (2007), No. 1, 1-26.

[11] C. Khare, *Serre's modularity conjecture: the level one case*. Duke Math. J. **134** (2006), no.3, 557–589.

[12] S. Lang, *Introduction to Modular Forms*. Springer–Verlag, 1976.

[13] D.A. Marcus, *Number Fields*. Springer–Verlag, 1977.

[14] J.–P. Serre, *Congruences et formes modulaires (d'après H.P.F. Swinnerton-Dyer)*. Sém. Bourbaki 1972/72, no. **416**.

[15] J.–P. Serre, *Corps Locaux*. Hermann, Quatrième édition, corrigée, 2004.

[16] J.–P. Serre, *A Course in Arithmetiic*. Springer-Verlag, 1973.

[17] J.–P. Serre, *Modular forms of weight one and Galois representations*. Algebraic Number Fields, Edited by A. Fröhlich, 193–268. Acad. Press, 1977.

[18] G. Wiese, *Dihedral Galois representations and Katz modular forms*. Documenta Math. **9** (2004), 123–133.

Universität Heidelberg
IWR, Im Neuenheimer Feld 368
69120 Heidelberg, Germany
E-mail : tommaso.centeleghe@iwr.uni-heidelberg.de
URL: http://www.iwr.uni-heidelberg.de/groups/arith-geom/centeleghe/