Tommaso Giorgio CENTELEGHE

Computing the number of certain Galois representations mod $p$


<http://jtnb.cedram.org/item?id=JTNB_2011__23_3_603_0>
Computing the number of certain Galois representations mod $p$

par Tommaso Giorgio CENTEGHE

1. Introduction

Let $p$ be a prime number and $\mathbb{F}_p$ an algebraic closure of the finite field with $p$ elements. Let $G_{\mathbb{Q}}$ denote the absolute Galois group of $\mathbb{Q}$, with respect to the choice of an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. 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 $\rho : G_{\mathbb{Q}} \to \text{GL}_2(\mathbb{F}_p)$ that are irreducible, odd, and unramified outside $p$.

Continuity in this context means that $\rho$ has open kernel; compactness of $G_{\mathbb{Q}}$ implies that $\rho$ has finite image, and there exists a finite extension $\mathbb{F}(\rho)$ of $\mathbb{F}_p$ for which a model of $\rho$ over $\mathbb{F}(\rho)$ can be found. The statement obtained from Theorem 1.1 replacing $\mathbb{F}_p$ by a finite subfield $\mathbb{F}$ 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 $\mathbb{F}$ of $\mathbb{F}_p$ so that all the representations considered can be realized over $\mathbb{F}$.

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 $T^0_k$ (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,
Computing Galois representations mod \( p \)

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 \( SL_2(\mathbb{Z}) \) 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 \( SL_2(\mathbb{Z}) \), and let \( M_k^0 \) be its cuspidal subspace. Denote by \( M_k(\mathbb{Z}) \) (resp. \( M_k^0(\mathbb{Z}) \)) 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 \( M_k(\mathbb{Z}) \subset M_k \) and \( M_k^0(\mathbb{Z}) \subset M_k^0 \) induce isomorphisms \( M_k(\mathbb{Z}) \otimes \mathbb{C} \simeq M_k \) and \( M_k^0(\mathbb{Z}) \otimes \mathbb{C} \simeq M_k^0 \). One way to see this is by first observing that \( M_k \) admits a \( \mathbb{C} \)–basis given by certain monomials in the Eisenstein series \( E_4 \) and \( E_6 \), whose expansions at infinity lie in \( \mathbb{Q} \otimes \mathbb{Z}[[q]] \) (cf. [12], I Thm. 2.2 and X §3, or [16], VII §3 Cor. 2 and §4), and then conclude by arguing that the \( \mathbb{Z} \)–rank of \( M_k(\mathbb{Z}) \) cannot exceed the dimension of \( M_k \).

Let \( p \) be a prime number. Following [14], we define the space \( M_k(F_p) \) of modular forms mod \( p \) of weight \( k \) on \( SL_2(\mathbb{Z}) \) to be \( M_k(\mathbb{Z})/pM_k(\mathbb{Z}) \), similarly the cuspidal subspace is \( M_k^0(F_p) = M_k^0(\mathbb{Z})/pM_k^0(\mathbb{Z}) \). 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 \( \mathbb{Z} \) (cf. [16], VII §5).

By definition, the Hecke ring \( T_k^0 \) is the subring of \( \text{End}_\mathbb{C}(M_k^0) \) generated by all the operators \( T_n \), for \( n > 0 \), and the Hecke algebra \( (T_k^0)_\mathbb{C} \) is the smallest \( \mathbb{C} \)–subalgebra of \( \text{End}_\mathbb{C}(M_k^0) \) containing all the \( T_n \)’s.
For every \( n \), the operator \( T_n \) is a semi–simple endomorphism preserving the integral structure \( \text{M}_k^0(\mathbb{Z}) \). Moreover, the algebra \( (\text{T}_k)^0 \) acts on \( \text{M}_k^0 \) 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

\[
\theta_k : T_k^0 \longrightarrow \prod_{1 \leq i \leq r} O_i
\]

which has finite cokernel. The \( \mathbb{Z} \)-rank of \( T_k^0 \) is equal to \( \text{dim}_\mathbb{C}(\text{M}_k^0) \).

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

If \( \theta_{k,i} : T_k^0 \rightarrow O_i \) denotes the composition of \( \theta_k \) with the projection onto \( O_i \), then all the systems of eigenvalues arising from \( \text{M}_k^0 \) are described by \( (\sigma(\theta_{k,i}(T_\ell))) \), where \( 1 \leq i \leq r \) and \( \sigma \in G_Q \) is any element (each \( K_i \) is considered as a subfield of \( \mathbb{C} \)).

Let us remark that in all known examples \( r \) is equal to 1 and the systems of eigenvalues arising from \( \text{M}_k^0 \) form a unique Galois orbit. Maeda’s conjecture is the statement that this happens for all \( k \).

The Hecke ring \( T_k^0 \) acts naturally on the space \( \text{M}_k^0(F_p) \) and, by extension of scalars, on \( \text{M}_k^0(F_p) \otimes F_p \), denoted by \( \text{M}_k^0(F_p) \) in what follows. A system of eigenvalues mod \( p \) arising from \( \text{M}_k^0(F_p) \) is a collection \( \Phi = (a_\ell)_{\ell \neq p} \) of elements \( a_\ell \in F_p \), indexed by primes \( \ell \neq p \), so that there exists a nonzero form \( f \in \text{M}_k^0(F_p) \) 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 \( f \in \text{M}_k^0(F_p) \) giving rise to \( \Phi \) that is an eigenvector for \( T_p \). Therefore there is a ring homomorphism \( \lambda_\Phi : T_k^0 \rightarrow F_p \) defined by \( T(f) = \lambda_\Phi(T)f \), for \( T \in T_k^0 \). The \( p \)-th eigenvalue \( a_p \), and hence the morphism \( \lambda_\Phi \), 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 \( \text{M}_k^0(F_p) \) and the set of \( F_p \)-valued points of \( \text{Spec}(T_k^0) \).

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

\[
\rho_\Phi : G_Q \longrightarrow \text{GL}_2(F_p),
\]
which is odd, unramified outside \( p \), and that is characterized by the equalities
\[
\text{tr}(\rho_{\Phi}(\text{Frob}_\ell)) = a_\ell, \quad \det(\rho_{\Phi}(\text{Frob}_\ell)) = \ell^{k-1},
\]
for all primes \( \ell \neq p \), where \( \text{Frob}_\ell \) is a Frobenius element of \( G_{\mathbb{Q}} \) at \( \ell \) (cf. [6], §11 Prop. 11.1).

If \( h \in \mathbb{Z}_{\geq 0} \) is a nonnegative integer then it follows from the theory of the \( \theta \)–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 \( M_{0}^{0}(\mathbb{F}_p) \), denoted by \( \Phi(h) \). We have
\[
\rho_{\Phi(h)} \simeq \chi_p^h \otimes \rho_{\Phi},
\]
where \( \chi_p : G_{\mathbb{Q}} \to \mathbb{F}_p^* \) is the mod \( p \) cyclotomic character, and \( \Phi(h) \) is usually called the \( h \)–fold twist of \( \Phi \).

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 \( \Phi \) is a system of mod \( p \) eigenvalues arising from \( M_{0}^{0}(\mathbb{F}_p) \), then there exists a twist \( \Phi(h) \) that arises from \( M_{k'+h}^{0}(\mathbb{F}_p) \), where \( 2 \leq k' \leq p+1 \).

In the weight range \( 2, 3, \ldots, p+1 \), and when \( \rho_{\Phi} \) 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 \( \rho_{\Phi} \) to a decomposition subgroup \( D_p < G_{\mathbb{Q}} \) at \( p \), is determined on the inertia subgroup by the (unique) eigenvalue \( a_p \) associated to \( \Phi \). We only point out that \( a_p \neq 0 \) if and only if \((\rho_{\Phi})_p\) is reducible.

Let \( \Phi \) be a system of eigenvalues mod \( p \), and assume that \( \rho_{\Phi} \) 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 \( \Phi \) be a system of eigenvalues arising from \( M_{k}^{0}(\mathbb{F}_p) \), where \( 2 \leq k \leq p+1 \), and so that \( \rho_{\Phi} \) 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 \( M_{p+3-k}^{0}(\mathbb{F}_p) \);

ii) \( \Phi(1-k) \) arises from \( M_{p+1-k}^{0}(\mathbb{F}_p) \).

From the description of \((\rho_{\Phi})_p\) given by the theorems of Deligne and Fontaine mentioned above, and from an elementary analysis of the \( \theta \)–cycle of \( \Phi \) (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 \( \mathcal{E}^{\text{irr}}(p) \) be the set of all systems \( \Phi = (a_\ell)_{\ell \neq p} \) of Hecke eigenvalues mod \( p \) arising from \( M^0_k(F_p) \), for some \( k \), so that the associated Galois representation \( \rho_\Phi \) is irreducible. By the level one case of Serre’s Conjecture, proved by Khare in 2005 (cf. [11]), the cardinality of \( \mathcal{E}^{\text{irr}}(p) \) is equal to the integer \( R(p) \) defined in the Introduction.

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

\[
R(p) = |\mathcal{E}^{\text{irr}}(p)| \leq (p-1) \sum_{2 \leq k \leq p+1} \dim_{C}(M^0_k).
\]

Let \( U(p) \) be the upper bound for \( R(p) \) given by inequality (3.1). Using the well–known formulas for \( \dim_{C}(M^0_k) \) (cf. [12], p. 12), one finds that there is an explicit degree 3 polynomial \( F_\alpha(x) \in \mathbb{Q}[x] \), depending only on the residue class \( \alpha \) 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

\[
U(p) \sim p^3/48 + O(p^2).
\]

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 \( \geq 11 \). 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, $\delta_R$ denotes the discriminant of a finite $\mathbb{Q}$-ring $R$ (cf. §4).

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

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

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

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

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

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

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

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

From Theorem 2.3 we deduce the formula

$$(3.3) \quad |E^{\text{irr}}(p)| = (p-1) \sum_{2 \leq k \leq p+1} \left[ |E(p, k)| - |E^{\text{Eis}}(p, k)| - \frac{1}{2} |E^{p-\text{tame}}(p, k)| \right]$$

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

### 3.1. Computation of $|E^{\text{Eis}}(p, k)|$.

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 $M_k^0(\mathbb{F}_p) \neq 0$. Then $E^{\text{Eis}}(p, k)$ is not empty if and only if $p$ divides the numerator of the $k$-th Bernoulli number $b_k$. Moreover, if $E^{\text{Eis}}(p, k)$ 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 $M_k^0(\mathbb{F}_p) = 0$. 

\[\square\]
3.2. Computation of $|\mathcal{E}(p,k)|$. Let $k$ be a weight $\leq p+1$, and $n_k$ the integer $\dim_{\mathbb{F}_p}(M_k^0(\mathbb{F}_p)) = \dim_{\mathbb{C}}(M_k^0)$. 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, $T_r \in T_k^0$ the $r$–th Hecke operator, and $h_r(x) \in \mathbb{Z}[x]$ its characteristic polynomial as an endomorphism of $M_k^0(\mathbb{C})$. Assume that the discriminant $\delta_r$ of $h_r(x)$ is nonzero. Let $f_p^{(r)}$ be the number of $\mathbb{F}_p$–valued points of the spectrum of the ring $\mathbb{Z}[T_r] \simeq \mathbb{Z}[x]/(h_r(x))$, then

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

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

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

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

$$\mathbb{F}_p[x]/(\bar{h}_r(x)) \simeq T_k^0/pT_k^0,$$

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 $\mathbb{Z}[T_r] \subset \text{End}_\mathbb{C}(M_k^0)$ is isomorphic to $\mathbb{Z}[x]/(h_r(x))$ 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 $r > 1$. 
Computing Galois representations mod $p$

Consider all pairs $(p, k)$, where $p$ is a prime number $\leq 2593$, 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.

<table>
<thead>
<tr>
<th>$r$</th>
<th>2</th>
<th>3</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>10</th>
<th>11</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>222370</td>
<td>256</td>
<td>36</td>
<td>5</td>
<td>13</td>
<td>2</td>
<td>4</td>
<td>2</td>
</tr>
</tbody>
</table>

Table 3.1. 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 $n_k - |E(p, k)|$.

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 $M_{(p+1)/2}^0$ 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 $|E(p, k)|$ in these cases. As it turns out, in all these cases we have $|E(p, k)| = n_k$.

Overall we found that $n_k - |E(p, k)|$ 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.

<table>
<thead>
<tr>
<th>$t$</th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>${(p, k) \mid n_k - E(p, k) = t}$</td>
<td>222171</td>
<td>198</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 3.2. Number of pairs $(p, k)$ such that $n_k - |E(p, k)| = t$

Remark. Let $\tilde{T}_k^0$ be the integral closure of the Hecke ring $T_k^0$ in $T_k^0 \otimes \mathbb{Q}$. For all the pairs $(p, k)$ considered, $p$ does not divide the index of $T_k^0$ in $\tilde{T}_k^0$. 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 $|E(p, k)| = n_k$ in the remaining 13 cases. The conclusion is that, if $k \leq p + 1$ and $p \leq 2593$, we have $\text{Hom}_{\text{rings}}(T_k^0, \mathbb{F}_p) = \text{Hom}_{\text{rings}}(\tilde{T}_k^0, \mathbb{F}_p)$, 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 $T_k^0$ 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 $T_k^0 \otimes \mathbb{Q}$.

### 3.3. An upper bound for $|\mathcal{E}^{p\text{-tame}}(p, k)|$.

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

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

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

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

**Proof.** Let $\Phi = (a_q)_{q \neq p}$ be a system of eigenvalues arising from $M_k^0(\mathbb{F}_p)$ so that $\rho_\Phi$ is irreducible. By the tameness criterion established by Gross (cf. Thm. 2.3 ii)), the restriction of $\rho_\Phi$ 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 $M_{p+1-k}^0(\mathbb{F}_p)$ so that

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

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

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

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

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

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

$$|\mathcal{E}^{p\text{-irr}}(p, k)| \leq e_p(h, j).$$
For any given prime $\ell \neq p$, the two propositions provide upper bounds for $|E^{p-\text{split}}(p,k)|$ and $|E^{p-\text{irr}}(p,k)|$. 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 $|E^{p-\text{split}}(p,k)|$ (resp. $|E^{p-\text{irr}}(p,k)|$) we considered the Hecke operator $T_{\ell_0}$, where $\ell_0$ is smallest prime $\ell \neq p$ that is not a quadratic residue mod $p$, for otherwise the characteristic polynomials of $T_\ell$ 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 $\dim \mathbb{C}(M_k^0)$, the worst possible.

**Remark.** The upper bounds for $|E^{p-\text{split}}(p,k)|$ and $|E^{p-\text{irr}}(p,k)|$ obtained with the methods of Propositions 3.3 and 3.4 turned out to be reasonably small. We find for example that $|E^{p-\text{split}}(p,k)|$ is zero for 221984 pairs $(p,k)$ out of the total 222370 analyzed, and that $|E^{p-\text{irr}}(p,k)|$ 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 $\mathbb{Q}$ (up to twisting by the mod $p$ cyclotomic character), that are tamely ramified.

If $h$ is the class number of $\mathbb{Q}(\sqrt{-p})$, then for $p \equiv 3 \mod 4$ and $k = (p + 1)/2$ it can be shown that the set $E^{p-\text{split}}(p,k)$ contains precisely $(h - 1)/2$ eigensystems $\Phi$ 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 $E^{p-\text{split}}(p,(p + 1)/2) \geq (h - 1)/2$.

Summarizing, we observe that if $p$ is a prime for which we find that $E^{p-\text{irr}}(p,k)$ is empty for all $k \leq p + 1$, and that the union of the sets $E^{p-\text{split}}(p,k)$ 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 $\Phi$ be a system of mod $p$ eigenvalues arising from $M_k^0(\mathbb{F}_p)$ so that $\rho_\Phi$ is of **dihedral type**, meaning that the projective image $G$ of $\rho_\Phi$ in $\text{PGL}_2(\mathbb{F}_p)$ is isomorphic to a dihedral group $C_n \rtimes \mathbb{Z}/2\mathbb{Z}$, where $C_n$ is a cyclic group of order $n \geq 2$ and the nontrivial element of $\mathbb{Z}/2\mathbb{Z}$ acts on $C_n$ by inversion. Since $\rho_\Phi$ is, by definition, semi–simple, it follows that any representation $\rho_\Phi$ 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 $\Phi$ be an eigensystem arising from $M_k^0(\mathbb{F}_p)$, with $2 \leq k \leq p + 1$. The representation $\rho_\Phi$ is of dihedral type if and only if $\Phi = \Phi(p-1)/2$. In this case we have

i) $\rho_\Phi$ 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 $\chi_p \chi_p^{(p-1)/2}$, where $\chi_p$ denotes the mod $p$ cyclotomic character of $G_p = G(\mathbb{Q}_p/\mathbb{Q})$;
iv) the image of $\rho \Phi$ is isomorphic to $C_n \rtimes \mathbb{Z}/2\mathbb{Z}$, with $n$ odd;
v) $\rho \Phi = \text{Ind}^Q_K(\Psi)$, where $K = \mathbb{Q}(\sqrt{-p})$, and $\Psi : G_K \to \mathbb{F}_p^*$ is a continuous, everywhere unramified character.

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

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

4. Discriminants of $S_\mathbb{Q}$–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 $S_\mathbb{Q}$–ring if the following conditions are satisfied:

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

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

The rank of $R$ is its rank as a $\mathbb{Z}$–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 $\mathbb{Q}$. Our motivation for considering them is that the Hecke ring $\mathbb{T}^0_k$ is of this type.

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

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

$$R \otimes \mathbb{Q} \simeq \prod_{1 \leq i \leq r} K_i,$$

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

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

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

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

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

**Proposition 4.1.** Any finite $S\mathbb{Q}$–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 $\delta_R$ of a finite $S\mathbb{Q}$–ring $R$ is defined to be the determinant of the bilinear form

$$R \times R \ni (x, y) \rightarrow \text{tr}(xy) \in \mathbb{Z},$$

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

$$l_a : R \otimes \mathbb{Q} \rightarrow R \otimes \mathbb{Q}$$

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

$$(4.1) \quad \text{tr}(a) = \sum_\sigma \sigma(a),$$

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

If $R$ is the ring of integers of a number field $K$, then $\delta_R$ coincides with the discriminant $\delta_K$ of $K$.

The discriminant is multiplicative on any finite product of finite $S\mathbb{Q}$–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 $S\mathbb{Q}$–ring $R$, since $\delta_K \neq 0$ for any number field $K$. If $h(x) \in \mathbb{Z}[x]$ is a monic, square free polynomial of discriminant $\delta_h$, then $\delta_{R_h} = \delta_h$ (cf. [13], Chp. 2 Thm. 8).
5. Discriminants and $\mathbb{F}_p$-valued points of Spec($R$)

The goal of this section is to prove Theorem 5.1 which, for a finite $S_{\mathbb{Q}}$–ring $R$, gives a lower bound for the number of $\mathbb{F}_p$–valued points of 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 $\mathbb{Z}[T] \subset R$ to be prime to $p$.

For a prime number $p$, let $\nu_p$ denote the additive $p$–adic valuation of $\mathbb{Q}_p$, 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 $\mathbb{Q}$ and of discriminant $\delta_K$. If $p$ is any prime, let $f_p$ be the number of $\mathbb{F}_p$–valued points of 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 $p$ of $K$ above $p$, let $r_p$ and $e_p$ denote, respectively, the inertial degree and ramification index associated to $p$. There is the well–known formula (cf. [15], I §5, Prop. 10)

$$\sum_p e_p f_p = n$$

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

Let $K_p$ be the completion at $p$ of $K$ and $p^{\infty}$ be the different of the local extension $K_p/\mathbb{Q}_p$. We know that

$$r_p \geq e_p - 1,$$

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

$$\nu_p(\delta_K) = \sum_p f_p r_p.$$

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

$$\sum_p f_p r_p \geq \sum_p f_p (e_p - 1) = n - \sum_p f_p.$$

Moreover, equality holds if and only if every $p$ is tamely ramified above $p$, that is if and only if $p$ is tamely ramified in $K$. Observing that $\sum_p f_p = f_p$ concludes the proof of the lemma. $\square$

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 $p_0$ of $R$ above $p$ so that $p|e_{p_0}$ and, in the notation used in the proof of Lemma 5.1, $r_{p_0} > e_{p_0} - 1$. In particular

$$r_{p_0} > e_{p_0} - 1 \geq p - 1.$$  

By the proof of Lemma 5.1, we obtain

$$\nu_p(\delta_K) = \sum_p f_p r_p > p - 1,$$

which completes the proof of the corollary. \qed

Corollary 5.2. If $\nu_p(\delta_K) = 1$ then there exists exactly one prime $p_0$ of $R$ that lies above $p$ and that is ramified. We have $e_{p_0} = 2$, $f_{p_0} = 1$, and $\text{Spec}(R)$ has exactly $n - 1$ distinct $\mathbf{F}_p$-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 $\mathbf{F}_p$-valued points of $\text{Spec}(R)$ 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 $\sum f_p$ 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 $p_0$, and for which, moreover, we must have $e_{p_0} = 2$ and $f_{p_0} = 1$. \qed

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

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

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

Proof. The extension $R' \subset R$ is finite, therefore integral, and any $\mathbf{F}_p$-valued point of $\text{Spec}(R')$ can be lifted to one of $\text{Spec}(R)$ (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 $\iota$ 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 \( \mathbb{F}_p \), 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. \( \mathbb{F}_p \)), and let \((R/pR)_{\text{red}}\) (resp. \((R'/I)_{\text{red}}\)) be the reduced ring associated to \( R/pR \) (resp. \( R'/I \)). We have the following exact sequences of \( \mathbb{F}_p \)-vector spaces:

\[
0 \rightarrow \sqrt{0} \rightarrow R/pR \rightarrow (R/pR)_{\text{red}} \rightarrow 0,
\]
\[
0 \rightarrow \sqrt{0}' \rightarrow R'/I \rightarrow (R'/I)_{\text{red}} \rightarrow 0.
\]

Now, the injection \( R' \rightarrow R/p \) induces the inclusions

\[
\sqrt{0}' \subset \sqrt{0} \quad \text{and} \quad (R'/I)_{\text{red}} \subset (R/pR)_{\text{red}}.
\]

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 \( S_\mathbb{Q} \)-ring of rank \( n \). If \( p \) is any prime number, let \( f_p \) denote the number of \( \mathbb{F}_p \)-valued points of \( \text{Spec}(R) \). Then

\[
f_p \geq n - \nu_p(\delta_R).
\]

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

**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 \( S_\mathbb{Q} \)-rings. Therefore the inequality

\[
f_p \geq n - \nu_p(\delta_R)
\]

holds for any finite \( S_\mathbb{Q} \)-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 \( S_\mathbb{Q} \)-ring \( R \) that is integrally closed in \( R \otimes \mathbb{Q} \). In this case the second part of the theorem follows immediately from Lemma 5.1.

Let now \( R \) be any finite \( S_\mathbb{Q} \)-ring, let \( \bar{R} \subset R \otimes \mathbb{Q} \) be its integral closure, and let \( d \) be the (finite) index \([\bar{R} : R]\). If \( \bar{f}_p \) denote the number of \( \mathbb{F}_p \)-valued
Computing Galois representations mod $p$ points of $\text{Spec}(\tilde{R})$, 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

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

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 $\mathbb{F}_p$–valued points of $\text{Spec}(R)$ in terms of numerical data encoded in the characteristic polynomial of an element $T \in R$ that generates a finite index subring $\mathbb{Z}[T] \subset R$. It will be useful in our computations when $R$ is a Hecke ring $\mathbb{T}_k$ and $T$ is an Hecke operator $\mathbb{T}_\ell$.

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

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

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

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

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

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

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

Notice that $f_p^{(h)}$ is simply the number of distinct roots in $\mathbb{F}_p$ 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 $S_\mathbb{Q}$–ring and has no nilpotent elements. It follows that the endomorphism of $R \otimes \mathbb{Q}$ 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 $\mathbb{Z}[T]$ has rank $n$ as an abelian group, hence the index $[R : \mathbb{Z}[T]]$ 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

$$f_p \geq f_p(h) \geq f_p - \nu_p(d) \geq n - \nu_p(\delta_R) - \nu_p(d) \geq n - \nu_p(\delta_h).$$

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 $\mathbb{Z}[T]$ 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 $[R : \mathbb{Z}[T]]$. Replacing $R$ by its integral closure $\tilde{R}$ and reasoning as above we easily see that $p$ does not divide $[\tilde{R} : \mathbb{Z}[T]]$, and the proposition follows. \hfill \Box

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 $\tilde{R} \otimes \mathbb{Q}$ 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

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

where $\mathcal{E}(p, k)$, $\mathcal{E}^{\text{Eis}}(p, k)$ and $\mathcal{E}^{p-\text{tame}}(p, k)$ are, respectively, the set of systems of eigenvalues mod $p$ arising from the Hecke module $M^0_k(F_p)$; its subset given by those eigensystems $\Phi$ for which the associated mod $p$ Galois representation $\rho_\Phi$ of $\mathbb{Q}$ is reducible; and the subset of the $\Phi$ such that $\rho_\Phi$ 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 $\mathcal{E}^{\text{Eis}}(p, k)$, and in subsection 3.3 we explained how we obtained an upper bound for the size of $\mathcal{E}^{p-\text{tame}}(p, k)$, which is the disjoint union of $\mathcal{E}^{p-\text{split}}(p, k)$ and $\mathcal{E}^{p-\text{irr}}(p, k)$ (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 $|\mathcal{E}^{p-\text{tame}}(p, k)|$ 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 $\sum_{2 \leq k \leq p + 1} |\mathcal{E}^{\text{Eis}}(p, k)|$, which gives the total number of systems of eigenvalues mod $p$ corresponding to reducible representations, and arising from the spaces $M^0_k(F_p)$, where $k \leq p + 1$;

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

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

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

($\Delta/p^2$): 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 $\rho$ of $\mathbb{Q}$ of the type considered, such that $\rho$ is non–dihedral and the local representation $\rho_p$ is decomposable. Similarly, $u_b$ controls from above the number of Galois representations of $\mathbb{Q}$, 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 $\sum_{2 \leq k \leq p + 1} |\mathcal{E}^{p-\text{tame}}(p, k)|$, this in fact coincides with the number of representations $\rho$ 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.
<table>
<thead>
<tr>
<th>p</th>
<th>r</th>
<th>$u_a$</th>
<th>$u_b$</th>
<th>$L$</th>
<th>$\Delta/p^2$</th>
<th>p</th>
<th>r</th>
<th>$u_a$</th>
<th>$u_b$</th>
<th>$L$</th>
<th>$\Delta/p^2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>10*</td>
<td>0.0000</td>
<td>211</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0.0000</td>
</tr>
<tr>
<td>13</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>12*</td>
<td>0.0000</td>
<td>223</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>0.0111</td>
</tr>
<tr>
<td>17</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>48*</td>
<td>0.0000</td>
<td>227</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0.0131</td>
</tr>
<tr>
<td>19</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>72*</td>
<td>0.0000</td>
<td>229</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>0.0130</td>
</tr>
<tr>
<td>23</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>143*</td>
<td>0.0207</td>
<td>233</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0.0085</td>
</tr>
<tr>
<td>29</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>336*</td>
<td>0.0000</td>
<td>239</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0.0145</td>
</tr>
<tr>
<td>31</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>405*</td>
<td>0.0156</td>
<td>241</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>0.0123</td>
</tr>
<tr>
<td>37</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>720*</td>
<td>0.0262</td>
<td>251</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0.0059</td>
</tr>
<tr>
<td>41</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1080*</td>
<td>0.0000</td>
<td>257</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>3</td>
<td>0.0155</td>
</tr>
<tr>
<td>43</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1260*</td>
<td>0.0000</td>
<td>263</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>3</td>
<td>0.0189</td>
</tr>
<tr>
<td>47</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1656*</td>
<td>0.0208</td>
<td>269</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>0.0111</td>
</tr>
<tr>
<td>53</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2496*</td>
<td>0.0000</td>
<td>271</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>3</td>
<td>0.0202</td>
</tr>
<tr>
<td>59</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>3393*</td>
<td>0.0416</td>
<td>277</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>0.0035</td>
</tr>
<tr>
<td>61</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3900*</td>
<td>0.0000</td>
<td>281</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0.0000</td>
</tr>
<tr>
<td>67</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>5148*</td>
<td>0.0294</td>
<td>283</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>0.0158</td>
</tr>
<tr>
<td>71</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>6195*</td>
<td>0.0347</td>
<td>293</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>0.0136</td>
</tr>
<tr>
<td>73</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>6840*</td>
<td>0.0135</td>
<td>307</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>5</td>
<td>0.0146</td>
</tr>
<tr>
<td>79</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>8736*</td>
<td>0.0249</td>
<td>311</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>6</td>
<td>0.0240</td>
</tr>
<tr>
<td>83</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>10373*</td>
<td>0.0059</td>
<td>313</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>6</td>
<td>0.0031</td>
</tr>
<tr>
<td>89</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>12848*</td>
<td>0.0111</td>
<td>317</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>0.0031</td>
</tr>
<tr>
<td>97</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>16896*</td>
<td>0.0000</td>
<td>331</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>7</td>
<td>0.0135</td>
</tr>
<tr>
<td>101</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>19100*</td>
<td>0.0098</td>
<td>337</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>7</td>
<td>0.0000</td>
</tr>
<tr>
<td>103</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>20196*</td>
<td>0.0192</td>
<td>347</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>8</td>
<td>0.0086</td>
</tr>
<tr>
<td>107</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>22737*</td>
<td>0.0231</td>
<td>349</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>8</td>
<td>0.0028</td>
</tr>
<tr>
<td>109</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>24300*</td>
<td>0.0000</td>
<td>353</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>8</td>
<td>0.0141</td>
</tr>
<tr>
<td>113</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>27104*</td>
<td>0.0087</td>
<td>359</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>9</td>
<td>0.0124</td>
</tr>
<tr>
<td>127</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>38934*</td>
<td>0.0078</td>
<td>367</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>9</td>
<td>0.0054</td>
</tr>
<tr>
<td>131</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>42510*</td>
<td>0.0303</td>
<td>373</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0.0026</td>
</tr>
<tr>
<td>137</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>49368*</td>
<td>0.0000</td>
<td>379</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0.0118</td>
</tr>
<tr>
<td>139</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>50991*</td>
<td>0.0321</td>
<td>383</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>11</td>
<td>0.0104</td>
</tr>
<tr>
<td>149</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>63788*</td>
<td>0.0066</td>
<td>389</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>11</td>
<td>0.0076</td>
</tr>
<tr>
<td>151</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>66075*</td>
<td>0.0230</td>
<td>397</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>12</td>
<td>0.0050</td>
</tr>
<tr>
<td>157</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>74256*</td>
<td>0.0316</td>
<td>401</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>13</td>
<td>0.0049</td>
</tr>
<tr>
<td>163</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>83916*</td>
<td>0.0121</td>
<td>409</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>13</td>
<td>0.0024</td>
</tr>
<tr>
<td>167</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>90387*</td>
<td>0.0148</td>
<td>419</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>14</td>
<td>0.0095</td>
</tr>
<tr>
<td>173</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>100620*</td>
<td>0.0172</td>
<td>421</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>15</td>
<td>0.0047</td>
</tr>
<tr>
<td>179</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>111784*</td>
<td>0.0166</td>
<td>431</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>16</td>
<td>0.0138</td>
</tr>
<tr>
<td>181</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>115920*</td>
<td>0.0054</td>
<td>433</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>16</td>
<td>0.0115</td>
</tr>
<tr>
<td>191</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>130640*</td>
<td>0.0260</td>
<td>439</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>17</td>
<td>0.0124</td>
</tr>
<tr>
<td>193</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>140928*</td>
<td>0.0103</td>
<td>443</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>17</td>
<td>0.0022</td>
</tr>
<tr>
<td>197</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>150528*</td>
<td>0.0000</td>
<td>449</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>18</td>
<td>0.0044</td>
</tr>
<tr>
<td>199</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>154836*</td>
<td>0.0099</td>
<td>457</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>19</td>
<td>0.0043</td>
</tr>
</tbody>
</table>
\[
\begin{array}{ccccccccccc}
\text{ } & p & r & u_a & u_b & L & \Delta/p^2 & \text{ } & p & r & u_a & u_b & L & \Delta/p^2 \\
0.1 & 461 & 0 & 0 & 0.0021 & 739 & 0 & 0 & 0.0027 & 8281836 & 0.0027 \\
0.2 & 463 & 0 & 1 & 0.0075 & 743 & 0 & 1 & 0.0094 & 8414280 & 0.0094 \\
0.2 & 467 & 0 & 0 & 0.0096 & 751 & 1 & 2 & 0.0086 & 8690625 & 0.0086 \\
0.2 & 479 & 1 & 0 & 0.0187 & 757 & 1 & 0 & 0.0026 & 8904924 & 0.0026 \\
0.3 & 487 & 0 & 0 & 0.0051 & 761 & 1 & 0 & 0.0026 & 9047800 & 0.0026 \\
0.3 & 491 & 1 & 0 & 0.0182 & 769 & 0 & 0 & 0.0025 & 9337344 & 0.0025 \\
0.1 & 499 & 0 & 1 & 0.0049 & 773 & 1 & 1 & 0.0025 & 9484792 & 0.0025 \\
0.3 & 503 & 0 & 1 & 0.038 & 787 & 0 & 0 & 0.0012 & 10012854 & 0.0012 \\
0.1 & 509 & 0 & 0 & 0.000 & 797 & 1 & 0 & 0.0012 & 10401332 & 0.0012 \\
0.1 & 521 & 0 & 0 & 0.0038 & 809 & 2 & 0 & 0.0037 & 10878912 & 0.0037 \\
0.1 & 523 & 1 & 0 & 0.0057 & 811 & 1 & 0 & 0.0055 & 10958895 & 0.0055 \\
0.1 & 541 & 1 & 0 & 0.0036 & 821 & 1 & 0 & 0.0024 & 11373400 & 0.0024 \\
0.1 & 547 & 2 & 0 & 0.0063 & 823 & 0 & 0 & 0.0024 & 11457036 & 0.0024 \\
0.1 & 557 & 1 & 0 & 0.0035 & 827 & 1 & 0 & 0.0042 & 11624711 & 0.0042 \\
0.1 & 563 & 0 & 1 & 0.007 & 829 & 0 & 0 & 0.0000 & 11712060 & 0.0000 \\
0.1 & 569 & 1 & 0 & 0.0035 & 839 & 1 & 0 & 0.0142 & 12134302 & 0.0142 \\
0.1 & 571 & 0 & 0 & 0.0034 & 853 & 0 & 0 & 0.0011 & 12762960 & 0.0011 \\
0.1 & 577 & 1 & 1 & 0.0051 & 857 & 0 & 1 & 0.0023 & 12943576 & 0.0023 \\
0.1 & 587 & 2 & 0 & 0.007 & 859 & 0 & 0 & 0.0017 & 13035165 & 0.0017 \\
0.1 & 593 & 1 & 0 & 0.0016 & 863 & 0 & 0 & 0.0069 & 13215322 & 0.0069 \\
0.1 & 599 & 0 & 1 & 0.0066 & 877 & 1 & 0 & 0.0022 & 13874964 & 0.0022 \\
0.1 & 601 & 0 & 0 & 0.0033 & 881 & 1 & 0 & 0.0022 & 14066800 & 0.0022 \\
0.1 & 607 & 1 & 0 & 0.0065 & 883 & 0 & 0 & 1.0016 & 14163597 & 0.0016 \\
0.1 & 613 & 1 & 0 & 0.0016 & 887 & 1 & 0 & 0.0090 & 14352314 & 0.0090 \\
0.1 & 617 & 3 & 0 & 0.0064 & 907 & 0 & 0 & 0.0016 & 15355341 & 0.0016 \\
0.1 & 619 & 1 & 2 & 0.0064 & 911 & 0 & 1 & 0.0104 & 15553265 & 0.0104 \\
0.1 & 631 & 2 & 0 & 0.0079 & 919 & 0 & 1 & 0.0070 & 15970905 & 0.0070 \\
0.1 & 641 & 0 & 0 & 0.000 & 929 & 2 & 0 & 0.0021 & 16504480 & 0.0021 \\
0.1 & 643 & 0 & 1 & 0.0023 & 937 & 0 & 0 & 0.0000 & 16937856 & 0.0000 \\
0.1 & 647 & 3 & 0 & 1.0016 & 941 & 0 & 0 & 0.0000 & 17156880 & 0.0000 \\
0.1 & 653 & 1 & 0 & 0.0061 & 947 & 0 & 0 & 0.0010 & 17487756 & 0.0010 \\
0.1 & 659 & 1 & 0 & 0.0053 & 953 & 1 & 0 & 0.0020 & 17822392 & 0.0020 \\
0.1 & 661 & 0 & 0 & 0.006 & 967 & 0 & 0 & 0.0056 & 18619167 & 0.0056 \\
0.1 & 673 & 2 & 0 & 0.0029 & 971 & 1 & 0 & 0.0046 & 18853405 & 0.0046 \\
0.1 & 677 & 1 & 0 & 0.0044 & 977 & 0 & 0 & 0.0000 & 19210608 & 0.0000 \\
0.1 & 683 & 1 & 0 & 0.0043 & 983 & 0 & 1 & 0.0096 & 19558985 & 0.0096 \\
0.1 & 691 & 2 & 0 & 0.0057 & 991 & 0 & 1 & 0.0050 & 20046510 & 0.0050 \\
0.1 & 701 & 0 & 0 & 1.0014 & 997 & 0 & 0 & 0.0000 & 20418996 & 0.0000 \\
0.1 & 709 & 0 & 0 & 0.0014 & 1009 & 0 & 1 & 0.0029 & 21164976 & 0.0029 \\
0.1 & 719 & 0 & 0 & 1.0013 & 1013 & 0 & 0 & 0.0000 & 21422016 & 0.0000 \\
0.1 & 727 & 1 & 0 & 0.0054 & 1019 & 0 & 1 & 0.0058 & 21800470 & 0.0058 \\
0.1 & 733 & 0 & 1 & 0.0027 & 1021 & 0 & 0 & 0.0000 & 21935100 & 0.0000 \\
\end{array}
\]
<table>
<thead>
<tr>
<th></th>
<th>r</th>
<th>u_a</th>
<th>u_b</th>
<th>L</th>
<th>Δ/p^2</th>
<th></th>
<th>r</th>
<th>u_a</th>
<th>u_b</th>
<th>L</th>
<th>Δ/p^2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1031</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>22580175*</td>
<td>0.0082</td>
<td>1319</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>47392644*</td>
<td>0.0098</td>
</tr>
<tr>
<td>1033</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>22720512*</td>
<td>0.0000</td>
<td>1321</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>47622960*</td>
<td>0.0015</td>
</tr>
<tr>
<td>1039</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>23133665*</td>
<td>0.0062</td>
<td>1327</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>48273693*</td>
<td>0.0033</td>
</tr>
<tr>
<td>1049</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>23708588*</td>
<td>0.0009</td>
<td>1361</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>52095720*</td>
<td>0.0000</td>
</tr>
<tr>
<td>1051</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>23931600</td>
<td>0.0019</td>
<td>1367</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>52778142*</td>
<td>0.0073</td>
</tr>
<tr>
<td>1061</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>24622740</td>
<td>0.0028</td>
<td>1373</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>53468048</td>
<td>0.0029</td>
</tr>
<tr>
<td>1063</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>24758937</td>
<td>0.0061</td>
<td>1381</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>54429960</td>
<td>0.0021</td>
</tr>
<tr>
<td>1069</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>25187712</td>
<td>0.0009</td>
<td>1399</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>56586147</td>
<td>0.0053</td>
</tr>
<tr>
<td>1087</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>26484282</td>
<td>0.0027</td>
<td>1409</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>57820928*</td>
<td>0.0007</td>
</tr>
<tr>
<td>1091</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>26776940*</td>
<td>0.0045</td>
<td>1423</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>59561892*</td>
<td>0.0028</td>
</tr>
<tr>
<td>1093</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>26927628</td>
<td>0.0018</td>
<td>1427</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>60066865</td>
<td>0.0031</td>
</tr>
<tr>
<td>1097</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>27224640</td>
<td>0.0027</td>
<td>1429</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>60321576</td>
<td>0.0020</td>
</tr>
<tr>
<td>1103</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>27672873*</td>
<td>0.0049</td>
<td>1433</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>60835656*</td>
<td>0.0000</td>
</tr>
<tr>
<td>1109</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>28134336*</td>
<td>0.0000</td>
<td>1439</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>61588821</td>
<td>0.0079</td>
</tr>
<tr>
<td>1117</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>28747044</td>
<td>0.0017</td>
<td>1447</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>62631321*</td>
<td>0.0044</td>
</tr>
<tr>
<td>1123</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>29214636</td>
<td>0.0017</td>
<td>1451</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>63159100*</td>
<td>0.0020</td>
</tr>
<tr>
<td>1129</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>29684448</td>
<td>0.0035</td>
<td>1453</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>63423360</td>
<td>0.0006</td>
</tr>
<tr>
<td>1151</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>31449050*</td>
<td>0.0121</td>
<td>1459</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>64211049*</td>
<td>0.0023</td>
</tr>
<tr>
<td>1153</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>31627008*</td>
<td>0.0017</td>
<td>1471</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>65808225*</td>
<td>0.0044</td>
</tr>
<tr>
<td>1163</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>32459888*</td>
<td>0.0021</td>
<td>1481</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>67169800</td>
<td>0.0013</td>
</tr>
<tr>
<td>1171</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>33137325*</td>
<td>0.0012</td>
<td>1483</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>67440633</td>
<td>0.0023</td>
</tr>
<tr>
<td>1181</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>33992260</td>
<td>0.0042</td>
<td>1487</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>67980042*</td>
<td>0.0067</td>
</tr>
<tr>
<td>1187</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>34512784</td>
<td>0.0050</td>
<td>1489</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>68266464</td>
<td>0.0013</td>
</tr>
<tr>
<td>1193</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>35047184*</td>
<td>0.0008</td>
<td>1493</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>68822976*</td>
<td>0.0000</td>
</tr>
<tr>
<td>1201</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>35756400</td>
<td>0.0024</td>
<td>1499</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>69649510*</td>
<td>0.0039</td>
</tr>
<tr>
<td>1213</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>36846012*</td>
<td>0.0000</td>
<td>1511</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>71329380</td>
<td>0.0085</td>
</tr>
<tr>
<td>1217</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>37208384*</td>
<td>0.0032</td>
<td>1523</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>73062849*</td>
<td>0.0016</td>
</tr>
<tr>
<td>1223</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>37757967*</td>
<td>0.0069</td>
<td>1531</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>74219535*</td>
<td>0.0029</td>
</tr>
<tr>
<td>1229</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>38325880</td>
<td>0.0016</td>
<td>1543</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>75979377</td>
<td>0.0042</td>
</tr>
<tr>
<td>1231</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>38506995</td>
<td>0.0060</td>
<td>1549</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>76879872</td>
<td>0.0006</td>
</tr>
<tr>
<td>1237</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>39081084*</td>
<td>0.0016</td>
<td>1553</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>77474288</td>
<td>0.0025</td>
</tr>
<tr>
<td>1249</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>40234272</td>
<td>0.0007</td>
<td>1559</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>78363505*</td>
<td>0.0086</td>
</tr>
<tr>
<td>1259</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>41206419</td>
<td>0.0043</td>
<td>1567</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>79594299*</td>
<td>0.0022</td>
</tr>
<tr>
<td>1277</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>43008856</td>
<td>0.0015</td>
<td>1571</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>80206590*</td>
<td>0.0025</td>
</tr>
<tr>
<td>1279</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>43205985*</td>
<td>0.0050</td>
<td>1579</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>81442158</td>
<td>0.0018</td>
</tr>
<tr>
<td>1283</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>43618127*</td>
<td>0.0027</td>
<td>1583</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>82056758*</td>
<td>0.0050</td>
</tr>
<tr>
<td>1289</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>44237484*</td>
<td>0.0007</td>
<td>1597</td>
<td>1</td>
<td>3</td>
<td>0</td>
<td>84262416</td>
<td>0.0031</td>
</tr>
<tr>
<td>1291</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>44437920</td>
<td>0.0046</td>
<td>1601</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>84905600*</td>
<td>0.0006</td>
</tr>
<tr>
<td>1297</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>45067104*</td>
<td>0.0015</td>
<td>1607</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>85857563*</td>
<td>0.0040</td>
</tr>
<tr>
<td>1301</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>45485700*</td>
<td>0.0023</td>
<td>1609</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>86185584*</td>
<td>0.0012</td>
</tr>
<tr>
<td>1303</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>45694341</td>
<td>0.0034</td>
<td>1613</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>86831992*</td>
<td>0.0012</td>
</tr>
<tr>
<td>1307</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>46118125*</td>
<td>0.0034</td>
<td>1619</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>87799961</td>
<td>0.0040</td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>$p$</th>
<th>$r$</th>
<th>$u_a$</th>
<th>$u_b$</th>
<th>$L$</th>
<th>$\Delta/p^2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1621</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>88134480*</td>
<td>0.0006</td>
</tr>
<tr>
<td>1627</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>89116995</td>
<td>0.0015</td>
</tr>
<tr>
<td>1637</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>90775096</td>
<td>0.0012</td>
</tr>
<tr>
<td>1657</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>94151880</td>
<td>0.0006</td>
</tr>
<tr>
<td>1663</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>95171106</td>
<td>0.0042</td>
</tr>
<tr>
<td>1677</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>95868304*</td>
<td>0.0017</td>
</tr>
<tr>
<td>1699</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>96213576</td>
<td>0.0017</td>
</tr>
<tr>
<td>1709</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>101152832</td>
<td>0.0005</td>
</tr>
<tr>
<td>1721</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>105513400*</td>
<td>0.0011</td>
</tr>
<tr>
<td>1723</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>105880614</td>
<td>0.0017</td>
</tr>
<tr>
<td>1733</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>107737328</td>
<td>0.0023</td>
</tr>
<tr>
<td>1741</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>109245900*</td>
<td>0.0000</td>
</tr>
<tr>
<td>1747</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>110376882*</td>
<td>0.0017</td>
</tr>
<tr>
<td>1753</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>111523560*</td>
<td>0.0005</td>
</tr>
<tr>
<td>1759</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>112662309*</td>
<td>0.0048</td>
</tr>
<tr>
<td>1777</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>116175264*</td>
<td>0.0011</td>
</tr>
<tr>
<td>1783</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>117353610</td>
<td>0.0028</td>
</tr>
<tr>
<td>1787</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>118144793</td>
<td>0.0036</td>
</tr>
<tr>
<td>1789</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>118546188*</td>
<td>0.0022</td>
</tr>
<tr>
<td>1801</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>120958200*</td>
<td>0.0005</td>
</tr>
<tr>
<td>1811</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>122974115</td>
<td>0.0052</td>
</tr>
<tr>
<td>1823</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>125433768</td>
<td>0.0071</td>
</tr>
<tr>
<td>1831</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>127107225*</td>
<td>0.0035</td>
</tr>
<tr>
<td>1847</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>130463281*</td>
<td>0.0073</td>
</tr>
<tr>
<td>1861</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>133481404*</td>
<td>0.0005</td>
</tr>
<tr>
<td>1867</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>134777448*</td>
<td>0.0010</td>
</tr>
<tr>
<td>1871</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>135629230*</td>
<td>0.0064</td>
</tr>
<tr>
<td>1873</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>136086912*</td>
<td>0.0000</td>
</tr>
<tr>
<td>1877</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>136953628</td>
<td>0.0026</td>
</tr>
<tr>
<td>1879</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>137386029*</td>
<td>0.0045</td>
</tr>
<tr>
<td>1889</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>139610048*</td>
<td>0.0005</td>
</tr>
<tr>
<td>1901</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>142291000*</td>
<td>0.0010</td>
</tr>
<tr>
<td>1907</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>143639972</td>
<td>0.0026</td>
</tr>
<tr>
<td>1913</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>145006080</td>
<td>0.0015</td>
</tr>
<tr>
<td>1931</td>
<td>0</td>
<td>2</td>
<td>3</td>
<td>149133030</td>
<td>0.0051</td>
</tr>
<tr>
<td>1933</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>149612148*</td>
<td>0.0010</td>
</tr>
<tr>
<td>1949</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>153366040</td>
<td>0.0010</td>
</tr>
<tr>
<td>1951</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>153821850*</td>
<td>0.0056</td>
</tr>
<tr>
<td>1973</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>159108848</td>
<td>0.0020</td>
</tr>
</tbody>
</table>

- $p$ is the prime number.
- $r$ is a variable.
- $u_a$ and $u_b$ are variables.
- $L$ is a large number.
- $\Delta/p^2$ is the ratio of the change in $L$ to $p^2$.
Table 6.1. Table of results
Computing Galois representations mod $p$

References


Tommaso Giorgio Centeleghe
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/