# On $\ell$-adic representations and congruences for coefficients of modular forms

Susheel Shankar
Supervised by: Prof. Shaunak Deo

May 31, 2022

**Abstract**

The congruences between the Ramanujan tau function and other arithmetically interesting functions modulo primes are well studied. Using the relationship between $\ell$ adic representations and coefficients of modular forms conjectured by Serre and proved by Deligne, we prove that the set of primes modulo which such congruences can occur is a finite set. It is shown that 2,3,5,7,23 and 691 are the only primes for which there exist congruences for the tau function. The technique used can be applied to any cusp form of weight $k$ over the full modular group, which satisfy the hypotheses for the Serre-Deligne theorem. The set of these primes has been listed for five other cusp forms known to satisfy the hypotheses of the Serre-Deligne Theorem.

# 1 Introduction

Denote by $\mathcal{H}$ the upper half plane $\{z \in \mathbb{C}, \text{Im } z > 0\}$.

**Definition 1.1.** *Let $k$ be an integer. A meromorphic function $f : \mathcal{H} \to \mathbb{C}$ is said to be* **weakly modular of weight *k*** *if it satisfies the following condition:*

$$f(z) = (cz+d)^{-k} f(\frac{az+b}{cz+d}),\ \forall \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}).$$

It is easy to verify that a weakly modular function is $\mathbb{Z}$ periodic.

If the weakly modular function $f$ of weight $k$ is holomorphic on $\mathcal{H}$, then it can be shown using the $\mathbb{Z}$ periodicity that $f$ has a Laurent series expansion, $f(q) = \sum\limits_{n \in \mathbb{Z}} a_n q^n$, where $q = e^{2\pi i z}$ . (Notice that the map $z \mapsto e^{2\pi i z}$ takes $\mathcal{H}$ to the punctured unit disk $D^*$).

If $f(q)$ can be extended holomorphically to include the puncture, i.e if there exists a function $g$ holomorphic over the unit disk $D$ such that $g(q) = f(q)$ over $D^*$, then we say that $f$ is holomorphic at $\infty$.

**Definition 1.2.** *A weakly modular function of weight $k$ which is holomorphic over $\mathcal{H}$ and at $\infty$ is called a modular form of weight $k$.*

If $f$ is a modular form of weight $k$, then it follows from above that it has a fourier series expansion $f(q) = \sum\limits_{n=0}^{\infty} a_n q^n$. If $a_0 = 0$, then $f$ is called a **cusp form** of weight $k$.

Note: To be precise, the definition given above is for level 1 modular forms. Throughout this report, we shall be dealing with level 1 modular forms.

**Examples.**

1. $$\Delta = q \prod_{1}^{\infty} (1-q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n$$

   This is a cusp form of weight 12. In fact, it is the unique cusp form of weight 12 upto scaling.

   We define the Ramanujan $\tau$ function to be the map from $\mathbb{N}$ to $\mathbb{C}$ sending $n$ to $\tau(n)$.

2. $$E_{2v} = 1 + \frac{4v}{-b_{2v}} \sum_{v=1}^{\infty} \sigma_{2v-1}(n) q^n, \forall v \geq 2,$$

   where $b_{2v}$ denotes the $2v^{th}$ Bernoulli number, and $\sigma_t(n)$ denotes the sum of the $t^{th}$ powers of all positive divisors of $n$, i.e. $\sigma_t(n) = \sum\limits_{d|n, d \in \mathbb{N}} d^t$. The above modular forms are called the Eisenstein series of weight $2v$.

Congruences between $\tau(n)$ and $\sigma_v(n)$ have been studied for a long time and one can find many such congruences in literature. These congruences are modulo some primes and their powers. For a list of such congruences, one can refer to [1]. We give one such congruence relation here:

$$\tau(n) \equiv \sigma_{11}(n) \text{ mod } 691$$

There is one question of interest that pertains to these congruences: for what primes can one expect to find such congruence relations? . Answering this question is precisely the aim of this thesis.

In order to formulate a solution to this question, the theory of $\ell-$adic Galois representations is used. In the next section, the necessary tools from the theory of Galois Representations will be outlined.

## 2 Deligne's Theorem

In order to find the only primes for which the congruences exist, one needs to have some control over the types of primes for which congruences can occur. This is established by using a theorem proved by Deligne, which links the $\ell-$adic Galois representations and the coefficients of modular forms.

Let $\ell$ be a prime number and $K_\ell$ be the maximal algebraic extension of $\mathbb{Q}$ ramified only at $\ell$ and $\infty$.

**Theorem 2.1.** *(Serre-Deligne) (Theorem 1 in [1]) Let $f = \sum a_n q^n$ be a cusp form of weight $k$ for the full modular group, and suppose $a_1 = 1$, that every $a_n$ is in $\mathbb{Z}$, and the associated Dirichlet series has an Euler product*

$$\Sigma a_n n^{-s} = \Pi(1 - a_p p^{-s} + p^{k-1-2s})^{-1}.$$

*Then there is a continuous homomorphism*

$$\rho_{f,\ell} : Gal(K_\ell/\mathbb{Q}) \to GL_2(\mathbb{Z}_\ell)$$

*depending on $f$ such that for every Frobenius element $F_p$ corresponding to a prime $p \neq \ell$, $\rho_{f,\ell}(F_p)$ has the characteristic polynomial $x^2 - a_p x + p^{k-1}$.*

Note: We only state a special case of the theorem here, which will suffice for our purposes. For a statement of the actual theorem, the reader may refer to [2].

In particular, this theorem shows that det $\circ\, \rho_{f,\ell} = \chi_\ell^{k-1}$, the $(k-1)^{th}$ power of the $\ell-$adic cyclotomic character. When it is clear from the context what $f$ is, we will drop the subscript and denote the homomorphism by just $\rho_\ell$.

This theorem is useful in the following way: If the image of $\rho_\ell$ is small, then information about the determinant of the image of an element inside the Galois group can be used to extract information about the trace, thereby giving us the congruence relations we desire. As such, the next target would be to understand the image of $\rho_\ell$.

Let $G$ be the image of $\rho_\ell$. We say that $\ell$ is exceptional for the cusp form $f$ if the image of $\rho_\ell$ does not contain $SL_2(\mathbb{Z}_\ell)$. The following theorem helps us identify an exceptional prime.

**Theorem 2.2.** *Say $\ell > 3$, then $\ell$ is exceptional if and only if the image of $\tilde{\rho}_\ell$ does not contain $SL_2(\mathbb{F}_\ell)$. For $\ell = 2$ or 3, this is still a sufficient condition for $\ell$ to be exceptional for $f$. Here, $\tilde{\rho}_\ell$ denotes the induced map*

$$Gal(K_\ell/\mathbb{Q}) \to GL_2(\mathbb{Z}_\ell) \to GL_2(\mathbb{F}_\ell).$$

*The first arrow denotes $\rho_\ell$. The second map is obtained by going modulo $\ell$.*

For a proof, one may refer to the Corollary to Lemma 1 in [1].

The study of congruences is connected with the study of exceptional primes, which is shown later.

## 3 Possible images of $\tilde{\rho}_\ell$

As mentioned above, understanding the image of $\rho_\ell$ is useful in determining the primes for which congruence relations can occur. Lemma 3.3 will give a precise classification of the possible images of $\tilde{\rho}_\ell$. We first define a couple of special subgroups of $GL_2(\mathbb{F}_\ell)$.

**Definition 3.1.** *Any subgroup $H \subset GL_2(\mathbb{F}_\ell)$conjugate to the group of nonsingular upper triangular matrices inside $GL_2(\mathbb{F}_\ell)$ is said to be a Borel subgroup.*

**Definition 3.2.** *Any maximal semi-simple commutative subgroup of $GL_2(\mathbb{F}_\ell)$ is called a Cartan subgroup.*

We now classify the images of $\tilde{\rho}_\ell$ with the following lemma (Corollary 1 in [1]).

**Lemma 3.3.** *Let $\rho_\ell$ be any continuous homomorphism from $Gal(K_l/\mathbb{Q})$ to $GL_2(\mathbb{Z}_\ell)$ such that det $\circ\, \rho_\ell = \chi_\ell^{k-1}$ for some even integer $k$. Let $G \subset GL_2(\mathbb{F}_\ell)$ be the image of $\tilde{\rho}_\ell$ and let $H$ be the image of $G$ in $PGL_2(\mathbb{F}_\ell)$. Suppose that $G$ does not contain $SL_2(\mathbb{F}_\ell)$. Then one of the following cases hold:*

1. *$G$ is contained in a Borel subgroup of $GL_2(\mathbb{F}_\ell)$.*

2. *$G$ is contained in the normalizer of a Cartan subgroup, but is not in the Cartan Subgroup itself.*

3. *$H$ is isomorphic to the symmetric group $S_4$.*

It is evident that the cusp forms satisfying the hypotheses specified in Deligne's Theorem also satisfy the hypotheses in the above lemma. Thus, one can apply the results to such cusp forms. Combining the above theorem with Deligne's Theorem gives us the following result.

**Theorem 3.4.** *(Corollary 2 in [1]) Let $f = \Sigma a_n q^n$ be a cusp form of weight $k$ for the full modular group, such that it satisfies the hypotheses of Theorem 2.1; and let $\rho_\ell : Gal(K_\ell/\mathbb{Q}) \to GL_2(\mathbb{Z}_\ell)$ be the continuous homomorphism guaranteed by the Deligne's Theorem. Assume that the image of $\tilde{\rho_\ell}$ does not contain $SL_2(\mathbb{F}_\ell)$ (whence $\ell$ is an exceptional prime for $f$). Then the three cases in the above theorem correspond to the following congruences:*

1. *There is an integer $m$ such that $a_n \equiv n^m \sigma_{k-1-2m}(n)$ mod $\ell$ for all $n$ prime to $\ell$, where $\sigma_t(n)$ denotes the sum of the $t^{th}$ powers of the divisors of $n$.*

2. *$a_n \equiv 0$ mod $l$ whenever $n$ is a quadratic non-residue mod $\ell$.*

3. *$p^{1-k} a_p^2 \equiv 0, 1, 2$ or $4$ mod $\ell$, for all primes $p \neq \ell$.*

Henceforth, the exceptional primes $\ell$ which satisfy 1,2 or 3 in Theorem 3.4 will be called exceptional primes of type 1, type 2 or type 3, respectively.

# 4 The possible primes for which congruences can be obtained

It turns out that the only primes for which one can expect to find congruence relations for the coefficients of the cusp forms are the exceptional primes as defined in Section 2. As we shall see, there are only finitely many exceptional primes for any cusp form satisfying the hypotheses of Deligne's Theorem, and in fact, for $\Delta$ (which is known to satisfy these hypotheses), all the exceptional primes are known.

The following lemma implies that one cannot find congruence relations for the non exceptional primes:

**Lemma 4.1.** *Suppose that $f = \Sigma a_n q^n$ is a cusp form satisfying the conditions of Theorem 2.1 . Let $\ell$ be a prime which is not exceptional for $f$, and let $N, N^*$ be non-empty open sets in $\mathbb{Z}_\ell$ and $\mathbb{Z}_\ell^*$ respectively. Then the set of primes $p$ for which $p \in N^*$ and $a_p \in N$ has positive density*

*A brief sketch of the proof.* One first shows that the image of the map $(\rho_\ell, \chi_\ell) : \mathrm{Gal}(K_\ell/\mathbb{Q}) \to GL_2(\mathbb{Z}_\ell) \times \mathbb{Z}_\ell^*$, contains $SL_2(\mathbb{Z}_\ell) \times 1$. Using this, it can be shown that the image of the map above consists of all elements $\alpha \times \beta \in GL_2(\mathbb{Z}_\ell) \times \mathbb{Z}_\ell^*$ such that det $\alpha = \beta^{(k-1)}$. It therefore follows that $(\mathrm{Tr} \circ \rho_\ell, \chi_\ell) : \mathrm{Gal}(K_\ell/\mathbb{Q}) \to Z_\ell \times \mathbb{Z}_\ell^*$ is surjective (Tr stands for the trace). This map sends the Frobenius element associated to $p \neq l$ to $a_p \times p$. The theorem now follows because Frobenius elements are uniformly distributed in the Galois group. □

We therefore shift our focus to the exceptional primes. The following theorem, which is Lemma 8 in [1], helps us find a number that bounds the exceptional primes of types 1, 2 and 3.

**Theorem 4.2.** *Suppose $f$ is a cusp form that satisfies the various conditions specified in the Theorem 2.1. Let $\ell$ be a prime and $\rho_\ell$ be the map guaranteed by Theorem 2.1:*

1. *If $\ell$ is exceptional of type 1, then $\ell < k$ or $m = 0$ ($m$ as in Corollary 1) and $\ell$ divides the numerator of $b_k$.*

2. *If $\ell$ is exceptional of type 2, then $\ell < 2k$.*

3. *There are only finitely many exceptional primes of type 3.*

*Sketch of proof*

We only show 3 here: One can identify the exceptional primes of type 3 as follows. We pick a prime $p \neq 2$ such that $a_p \neq 0$. Then, if $\ell$ is exceptional of type 3, then from Theorem 3.4, either $\ell = p$ or $\ell$ divides one of $a_p^2, a_p^2 - p^{k-1}, a_p^2 - 2p^{k-1}, a_p^2 - 4p^{k-1}$.

Since k is even (there are no nontrivial modular forms of odd weight over the full modular group), none of the terms are zero, and hence the number of exceptional primes of type 3 is finite.

To prove 1 and 2, one uses the theory of modular forms mod $\ell$. The details have been omitted as they are too lengthy.

The above results can be restated as follows.

**Theorem 4.3.** *Given a modular form $f$ satisfying the hypotheses of Theorem 2.1, there are only finitely many primes which are exceptional for $f$.*

We can now classify the primes modulo whom one can obtain congruence relations for the coefficients. We just identify the exceptional primes of type 1,2 and 3, using the theorems above. The following corollary classifies them for six cusp forms which satisfy the hypotheses of Deligne's Theorem.

**Corollary 4.4.**

- *The exceptional primes of type 1 for the six cusp forms satisfying the Deligne's Theorem are given in the table below, along with the associated m value (m is as defined in Theorem 3.4)*

Table 1: Exceptional Primes of type 1

| Form | k | $\ell = 2$ | $\ell = 3$ | $\ell = 5$ | $\ell = 7$ | $\ell = 11$ | $\ell = 13$ | $\ell = 17$ | $\ell = 19$ | $\ell = 23$ | Other $\ell$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $\Delta$ | 12 | 0 | 0 | 1 | 1 | X | | | | | 691 |
| $E_4\Delta$ | 16 | 0 | 0 | 1 | 1 | 1 | X | | | | 3617 |
| $E_6\Delta$ | 18 | 0 | 0 | 2 | 1 | 1 | 1 | X | | | 43867 |
| $E_4^2\Delta$ | 20 | 0 | 0 | 1 | 2 | 1 | 1 | X | X | | 283 and 617 |
| $E_4R\Delta$ | 22 | 0 | 0 | 2 | 1 | X | 1 | 1 | X | | 131 and 593 |
| $E_4^2R\Delta$ | 26 | 0 | 0 | 2 | 2 | 1 | X | 1 | 1 | X | 657931 |

*The first two columns give the form and its weight, the last column consists of exceptional primes $\ell > k$ (we know $m = 0$ in this case). The other columns give the value of $m$ when $\ell < k$. Here, "X" means that the corresponding prime is not exceptional of type 1 for that cusp form.*

- *For the above six forms, the only exceptional primes of type 2 are $\ell = 23$ for $\Delta$ and $\ell = 31$ for $E_4\Delta$.*
- *With the possible exception of $\ell = 59$ for $E_4\Delta$, there are no exceptional primes of type 3 for any of these six forms.*

This theorem, combined with Lemma 4.1, gives us a list of possible primes for which one can expect to have congruence relations and also gives the description of congruences.

For a proof, one may refer to the corollary to Theorem 4 in [1].

# References

[1] Swinnerton-Dyer H.P.F. (1973), *On $\ell$-ADIC Representations and Congruences for Coefficients of Modular Forms. In: Kuijk W., Serre JP. (eds) Modular Functions of One Variable III.* Lecture Notes in Mathematics, vol 350. Springer, Berlin, Heidelberg

[2] Diamond, Fred. Shurman,Jerry, *A First Course in Modular Forms. Graduate texts in Mathematics*, Springer-Verlag (2000). ISBN 978-0-387-23229-4.