Modular forms of weight 1

Marios Magioladitis

Arbeitsgemeinschaft Galoisdarstellungen zu Modulformen

Institute of Experimental Mathematics (IEM)
University of Duisburg-Essen
Januar 2006

Arbeitsgemeinschaft Galoisdarstellungen zu Modulformen.
Organisation: G. Böckle, G. Frey, M. Möller. Wintersemester 2005/06.

Lecture **13. Modular forms of weight 1 (part 2)** was given on 24th January 2006 in the Institute of Experimental Mathematics (IEM).

I would like to thank Xavier Taixés for his help.

Marios Magioladitis
Homepage: http://www.exp-math.uni-essen.de/˜magiolad
E-mail: marios@math.uoc.gr

References

[DeSe] Delign, P. Serre, J.-P., Formes modulaires de poids 1, Ann. Sci. ENS. 7 No.4 (1974), 507-530. Available at: http://www.numdam.org/
[Fr] G. Frey (ed.), On Artin's conjecture for odd 2-dimensional representations, Lecture note in math. 1585 (1994), Springer-Verlag.

Contents

Chapter 1

Prelimaries

1.1 Elements of modular forms

Let N be an integer ≥ 1. We define

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}), a \equiv d \equiv 1(modN), b \equiv c \equiv 0(modN) \right\}$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}), a \equiv d \equiv 1(modN), c \equiv 0(modN) \right\}$$

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}), c \equiv 0(modN) \right\}$$

It's easy so see that

$$\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N)$$

Let f be a function over the semiplane $H = \{z \mid Im(z) > 0\}$. Let k be an integer and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be an element in $SL_2(\mathbb{Z})$. We write

$$(f \mid_k \gamma)(z) = (cz+d)^{-k} f(\gamma z), \text{ where } \gamma z = \frac{az+b}{cz+d}.$$

Definition 1.1.1. *Let Γ be a set such that $\Gamma(N) \subset \Gamma \subset SL_2(\mathbb{Z})$. A function f is called **modular of weight** k over Γ if:*

1. $f \mid_k \gamma = f \ \forall \gamma \in \Gamma$

2. *f is holomorphic in H*
3. *f is "holomorphic on points" i.e.* $\forall \sigma \in SL_2(\mathbb{Z})$ *the function* $f \mid_k \sigma$ *has a series development to powers of* $e^{2\pi z/N}$ *with exponents* ≥ 0.

If we replace "exponents ≥ 0*" with "exponents* > 0*", in the above then the modular form is called* ***parabolic***.

Definition 1.1.2. *Let* f *be a modular form of weight* k *over* $\Gamma_1(N)$ *and* $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$. *The form* $f \mid_k \gamma$ *depends only from the image of* d *in* $(\mathbb{Z}/N(\mathbb{Z})^*$. *We will note* $f \mid R_d$.
We also define $f \mid R_{-1} = (-1)^k f$.

Definition 1.1.3. *An homorphism*

$$\epsilon : (\mathbb{Z}/N(\mathbb{Z})^* \to \mathbb{C}^*$$

is called ***Dirichlet character*** *mod* N.
- ϵ *is called* ***even*** *if* $\epsilon(-1) = 1$.
- ϵ *is called* ***odd*** *if* $\epsilon(-1) = -1$.

Let k be an integer with the same parity with ϵ [i.e. $\epsilon(-1) = (-1)^k$]. A modular form is called of type (k, ϵ) over $\Gamma_0(N)$ if it is a modular form of weight k over $\Gamma_1(N)$ s.t.

$$f \mid R_d = \epsilon(d) f, \forall d \in (\mathbb{Z}/N(\mathbb{Z})^*,$$

i.e.

$$f\left(\frac{az+b}{cz+d}\right) = \epsilon(d)(cz+d)^k f(z), \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N).$$

We define

$$M_k(N, \epsilon) = \{f \text{ modular form of type } (k, \epsilon) \text{ over } \Gamma_0(N)\}$$

1.2 Elements of Galois Representation

Definition 1.2.1. *Let* G *be a topological group,* k *be a field with a topology and* V *be a* k*-vectorial space. Then a* ***linear representation*** *of* G *on* V *over* k *is a continuous homomorphism*

$$\rho : G \to GL_n(k).$$

We will say that ρ *is* ***simple*** *if* V *is a simple* G*-module. If* V *is a direct sum of simple* G*-modules, then we will say that* ρ *is* ***semi-simple***.

Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$ and $G = \text{Gal}\,(\overline{\mathbb{Q}}, \mathbb{Q})$.

The **Galois representations** of G are the linear representations.

$$\rho : G \to GL_n(k),$$

where k is one of the following:

(a) The field of complex numbers $\mathbb{C}$ with the discrete topology

(b) A finite field with the discrete topology

(c) A finite l-adic extension $\mathbb{Q}_l$ with the natural topology

In the first two cases, the image of ρ, $\rho(G)$, is finite. In the first case ρ is called **Artin representation**, in the second case **mod l representation** and in the third case **l-adic representation**.

Definition 1.2.2. *We call ρ **odd** if $det(\rho(c)) = 1$, where c is the complex conjucation.*

Definition 1.2.3. *A representation ρ is called **unramified** in a prime p if the image of the inertia group I_p is trivial. If ρ is unramified in p and ϕ_p ia a p-Frobenious we write $F_{\rho,p} := \rho(\phi_p(G))$. We denote then $P_{\rho,p}(T) := det(1 - F_{\rho,p}T)$.*

The following lemma results from Čebotarev's density theorem:

Lemma 1.2.4. *Let X be a set of prime numbers of density 1 and let ρ and ρ' be two semi-simple linear representations of G.*

If $\forall p \in X$, ρ and ρ' are unramified at p and $P_{\rho,p}(T) = P_{\rho',p}(T)$ (resp. $Tr(F_{\rho,p}) = Tr(F_{\rho',p})$ in the case that k has characteristic 0), then we have that ρ and ρ' are isomorphic.

Definition 1.2.5. *Let N be an integer ≥ 1 and X be the set of its prime divisors. If we choose ρ as above, we say that this representation is **unramified outside** N.*

Remark 1.2.6. *In the lemma above, if $k = \mathbb{C}$ the condition of semisimplicity is automatically satisfied.*

Chapter 2

Results

In this chapter we note $G = \mathrm{Gal}(\overline{\mathbb{Q}}, \mathbb{Q})$.

2.1 The main theorem

Theorem 2.1.1. *Let N be an integer ≥ 1, ϵ an odd Dirichlet character mod N and $f \in M_1(N, \epsilon)$ non-identically zero. We suppose that f is an eigenfunction of T_p, $p \not| N$ with eigenvalues a_p.*
It exists a linear representation

$$\rho : G \to GL_2(\mathbb{C})$$

which is unramified outside N and s.t. $Tr(F_{\rho,p}) = a_p$ and $\det(F_{\rho,p}) = \epsilon(p)$, $\forall p \not| N$. Moreover, ρ is irreducible $\Leftrightarrow$ f is a cusp form.

The proof is given in the last chapter.

Remark 2.1.2. *Čebotarev's density theorem implies that the representation ρ attached to f is unique up to isomorphism.*

Corollary 2.1.3. *The a_p's are sums of the roots of unity. In particular, $|a_p| \leq 2, \forall a_p$.*

Remark 2.1.4. *If the modular form is of weight 1 then its correspoding representation is odd.*

Proof. Omited. □

2.2 Artin conductor and local factors

Let l be a prime number. We choose an extension in $\overline{\mathbb{Q}}$ of the l-adic valuation of $\mathbb{Q}$.

Let

$$G_0 \supset G_1 \supset ... \supset G_i \supset ...$$

be the **ramifiction groups** of the image of ρ corresponding to this valuation.

We note V^{G_i} the subspace of V of the fixed elements by G_i.

We write

$$f_l(\rho) = \sum_{i=0}^{\infty} \left(\frac{G_i}{G_0} codim V^{G_i} \right),$$

where $codim V^{G_i} = \dim V - \dim V^{G_i}$.

From a theorem we have that $f_l(\rho) \in \mathbb{Z}_{\geq 0}$.

We define the **Artin conductor** to be

$$N_\rho = \prod_l l^{f_l(\rho)}.$$

Note that this is a finite product because ρ is ramified in finite many places and if ρ is unramified in a place l then $f_l(/rho) = 0$.

We will now give the definition the the Artin L-function.

Definition 2.2.1. *Let L/K be a finite normal extension of algebraic number fields and ρ be a representation of* $\mathrm{Gal}\,(L/K)$*. Let V be its corresponding vector space.*

For very prime ideal $\mathfrak{p}$ of K we choose a prive divisor $\mathfrak{P}$ in L. We note with $D_{\mathfrak{P}}$ the decomposition group and with $I_{\mathfrak{P}}$ the inertia group of $\mathfrak{P}$.

We note $V^{I_{\mathfrak{p}}}$ the subspace of V of the fixed elements by $I_{\mathfrak{p}}$. (Note that for almost all $\mathfrak{p}$ we have $V^{I_{\mathfrak{p}}} = V$).

Let $\sigma_{\mathfrak{P}}$ be the Frobenious automorphism i.e. the generator of $D_{\mathfrak{P}}/I_{\mathfrak{P}}$ which induces on the residual class field extension the automorphism

$$\overline{\sigma}_{\mathfrak{P}} : x \to x^q, x \in \mathfrak{O}_L/\mathfrak{P}, q = | \in \mathfrak{O}_K/\mathfrak{p}|.$$

$1 - N(\mathfrak{p})^{-s}/\sigma_{\mathfrak{p}}$ operates on $V^{I_{\mathfrak{p}}}$ and

$$L_{\mathfrak{p}}(s,\rho)^{-1} := \det_{V^{I_{\mathfrak{p}}}}(1 - N(\mathfrak{p})^{-s}\sigma_{\mathfrak{P}})$$

is a polynomial in $N(\mathfrak{p})^{-s}$ which does not depend of the choice of $\mathfrak{P}$.

*The **Artin L-function** of ρ is defined by*

$$L(s,\rho) := \prod_{\mathfrak{p}} L_{\mathfrak{p}}(s,\rho)$$

where the product runs over all the prime ideals of K.

Remark 2.2.2. *Brauer proved (1947) that the Artin L-function has a meromorphic continuation to the complex plane. Artin conjecture asserts that the Artin L-function is holomorphic to the whole plane with the exception a pole at $s = 1$ if ρ is trivial.*

We use the assumptions and the notation from theorem 2.1.1

Theorem 2.2.3. *Let f be a cusp newform with coefficients $a_n, n \geq 1$. Let ρ be the representation of G corresponding to f. We have:*

(a). The Artin conductor of ρ is equal to N.

(b). The Artin L-function $L(s,\rho)$ is equal to $\Phi_f(s) = \sum_{n=1}^{\infty} a_n n^{-s}$.

Corollary 2.2.4. *The representation ρ is ramified in all the prime divisors of N.*

Proof. Immediate from (a). □

Corollary 2.2.5. *$L(s,\rho)$ is an holomorphic function (in the whole plane).*

Proof. Immediate from (b). The Hecke theory shows that $\Phi_f(s)$ is holomorphic. □

The last corollary implies that the Artin conjecture is true in this certain case.

Proof. (Proof of theorem 2.2.3)
The proof uses the functional equation satisfied by $\Phi_f(s)$ and $L(s,\rho)$. For a proof see [DeSe] p.515-516. □

2.3 Characterisation of representations attached to forms of weight 1

We use the notation used in the first section of this chapter and we suppose that f is a cusp form.
The representation

$$\rho : G \to GL_2(\mathbb{C})$$

corresponding to f has the following properties:

(i) ρ is irreducible (results from the main theorem).

(ii) ρ is odd (see remark 2.1.4).

(iii) For every continuous character

$$\chi : G \to \mathbb{C}^*,$$

the Artin L-function $L(s, \rho \otimes \chi)$ is holomorphic (this is a result of corollary 2.2.5 to the cusp form $f_\chi = \sum \chi(n) a_n q^n$).

Reciprocally,

Theorem 2.3.1. *(Weil-Langlands) Let a representation $\rho : G \to GL_2(\mathbb{C})$ satisfying the conditions (i), (ii), (iii) above. We write*

$$L(s, \rho) = \sum a_n n^{-s}, f = \sum a_n q^n, \epsilon = det(\rho), N = conductor\ of\ \rho.$$

Then f is a cusp newform of type $(1, \epsilon)$ over $\Gamma_0(N)$, and ρ is the representation attached to f.

Remark 2.3.2. *This theorem can be generalized for all global fields.*

2.4 The Artin Conjecture for odd 2-dimensional representations

Let

$$PGL_2(\mathbb{C}) = GL_2(\mathbb{C})/\mathbb{C}^*.$$

Let $\rho : G \to GL_2(\mathbb{C})$ be an odd, irreducible representation. We may consider its projectivisation:

$$\overline{\rho} : G \to PGL_2(\mathbb{C}).$$

obtained by composing ρ with the canonical homomorphism. The image of $\overline{\rho}$, $\overline{\rho}(G)$, is a finite subgroup of $PGL_2(\mathbb{C})$ i.e. a priori is isomorphic to one of the following:

(a) A dihedral group (i.e. a non-trivial extension of a group of order 2 by a cyclic group).

(b) The symmetric A_4 group

(c) The symmetric S_4 group

(d) The symmetric A_5 group

The cyclic case is excluded because we assumed ρ to be irreducible.

Artin's conjecture has been proven for the dihedral case by Hecke.
If ρ is of dihedral type then is induced to a representation of degree 1 of the $\mathrm{Gal}\,(\overline{\mathbb{Q}}, \mathbb{Q}(\sqrt{d}))$, where $\mathbb{Q}(\sqrt{d})$ is a quadratic extension of $\mathbb{Q}$. The condition (iii) is then satisfied and ρ responds in a cusp form.

Langlands (1980) proved it for the A_4-type and Tunnell (1981) for the S_4-type.

The A_5 case is still open and so the question of displaying at least examples of representations of A_5-type whose Artin L-series are L-series of a newform of weight 1 arises. The question is considered difficult and till up to now we have only few examples. A method of producing such examples is described in [Fr].

Chapter 3

l-adic representation and representation mod l

In this chapter we note $G = \mathrm{Gal}\,(\overline{\mathbb{Q}}, \mathbb{Q})$.

3.1 l-adic representations

We will use the following result

Theorem 3.1.1. *Let $f \in M_k(N, \epsilon)$ non-identically zero. We suppose that $k \geq 2$ and f is an eigenfunction of the $T_p, p \not| N$, with eigenvalues a_p. Let K be a finite extension of $\mathbb{Q}$, containing the a_p's and $\epsilon(p)$'s. Let λ be a finite prime (place) of K of residual characteristic l and let K_λ be the completion of K in λ.*
It exists a continuous semi-simple linear representation

$$\rho_\lambda : G \to GL_2(K)$$

which is unramified outside Nl and s.t.

$$Tr(F_{\rho_\lambda, p}) = a_p \text{ and } det(F_{\rho_\lambda, p}) = \epsilon(p) p^{k-1} \text{ if } p \not| Nl$$

Due to Čebotarev's density theorem the last condition determines ρ_λ in a unique way, up to isomorphism.

Corollary 3.1.2. *Let $(f, N, k, \epsilon, (a_p))$ and $(f', N', k', \epsilon', (a'_p))$ be as in theorem 3.1.1. If the set of prime numbers p s.t. $a_p = a'_p$ has density 1, then $k = k', \epsilon = \epsilon'$ and $a_p = a'_p, \forall p \not| NN'$.*

Indeed, the representations attached to f and f' (for the same choice of K and λ) are isomorphic due to Čebotarev's density theorem (see also lemma 1.2.4).

Remark 3.1.3. *Once the main theorem is proven, it's easy to see that 3.1.1 and 3.1.2 also hold for weight 1; however in that case the image of group G is a finite group.*

3.2 Reduction mod l

Let $K \subset \mathbb{C}$ be a field of algebraic numbers, λ be a finite prime (place) of K, $\mathfrak{O}_\lambda$ be the corresponding valuation ring, $\mathfrak{m}_\lambda$ be it's corresponing maximal ideal, $k_\lambda = \mathfrak{O}_\lambda/\mathfrak{m}_\lambda$ be the residual field and l be the characteristic of k_λ.
To the following when we write mod λ we mean mod $\mathfrak{m}_\lambda$.

Definition 3.2.1. *Let $f \in M_k(N,\epsilon)$.*
*We say that f is **λ-integer** if the coefficients of the series f_∞ belong to $\mathfrak{O}_\lambda$.*
We say that $f \equiv 0$ (mod λ) if the coefficients of the series f_∞ belong to $\mathfrak{m}_\lambda$.
*We say that f is an **eigenvector** of T_p mod λ, of **eigenvalue** $a_p \in k_\lambda$, if we have*

$$f|T_p - a_p f \equiv 0 \ (mod\ \lambda).$$

Theorem 3.2.2. *With the above notations, let $f \in M_k(N,\epsilon), k \geq 1$, with coeffecients from K. We suppose that f is λ-integer, $f \not\equiv 0$ (mod λ), and f is an eigenvector of T_p mod λ, for $p \not| Nl$, with eigenvalues $a_p \in k_\lambda$. Let k_f be the subfield of k_λ containing the a_p's and the reductions mod λ of $\epsilon(p)$. Then it exists a semi-simple representation*

$$\rho : G \to GL_2(k_f)$$

which is unramified outside Nl and s.t. $\forall p \not| Nl$, we have that

$$Tr(F_{\rho,p}) = a_p \ and\ det(F_{\rho,p}) \equiv \epsilon(p)p^{k-1} \ (mod\ \lambda).$$

3.2.1 Proof of theorem 3.2.2

Let $(K', \lambda', f', k', \epsilon', (a'_p))$ be as in theorem 3.2.2, where $K' \supset K$ and λ' extends λ. If $a_p \equiv a'_p$ (mod λ') and $\epsilon(p)p^{k-1} \equiv \epsilon'(p)p^{k'-1}$ (mod λ'), $\forall p \not| Nl$, then the theorem for f is equivalent with the theorem for f'. The second condition is verified when $\epsilon = \epsilon'$ and $k \equiv k'$ (mod $l-1$) and then the first condition when $f \equiv f'$ (mod λ').

REDUCTION TO THE CASE $k \geq 2$.

For $n > 2$ even, let E_n be the Eisenstein series of weight n over $SL_2(\mathbb{Z})$ normalised s.t. the constant term is 1. If we choose n to be divisable by $l-1$, the developement of E_n is l-integer and $E_n \equiv 1 \pmod{l}$. (See [DeSe]). Then the product $f \cdot E_n$ is congruent to f mod λ, it's weight $k+n$ is congruent to k mod $(l-1)$.

This means that the theorem for f is equivalent to the theorem for $f \cdot E_n$, which has weight > 2.

REDUCTION IN THE CASE THAT f IS AN EIGENVECTOR OF T_p.

It suffices to verify that there exists a f' as the one in the begining of this paragraph, with $(k', \epsilon') = (k, \epsilon)$, which is an eigenvector of T_p.

That results from the following lemma applied to T_p, acting over the $\mathfrak{O}_\lambda$-module M of the modular form of type (k, ϵ) over $\Gamma_0(N)$ with coefficients in $\mathfrak{O}_\lambda$:

Lemma 3.2.3. *Let M be a finite free module over a d.v.r. $\mathfrak{O}$. We note with $\mathfrak{m}$ the maximal ideal of $\mathfrak{O}$, k its residual field, K the field of fractions. Let $\mathfrak{T}$ be a set of endomorphisms of M which is commutative. Let $f \in M/\mathfrak{m}M$ be an (common) eigenvector (non-zero) of $T \in \mathfrak{T}$, and $a_T \in k$ be the corresponding eigenvalues.*
It exists then a d.v.r. $\mathfrak{O}' \supset \mathfrak{O}$, with maximal ideal $\mathfrak{m}'$ s.t. $\mathfrak{O} \cap \mathfrak{m}' = \mathfrak{m}$, and its field of fractions K' is a finite extension of K, and exists a non-zero element f' of

$$M' = \mathfrak{O}' \otimes_{\mathfrak{O}} M,$$

which is an eigenvector of $T \in \mathfrak{T}$, with eigenvalues a'_T s.t. $a'_T \equiv a_T \pmod{\mathfrak{m}'}$.

Proof. Let $\mathfrak{H}$ be the subalgebra of $End(M)$ generated by $\mathfrak{T}$. Even by taking a finite extension of scalars, we can suppose that $K \otimes \mathfrak{H}$ is a product of Artin rings of the residual field K.

Let $\chi : \mathfrak{H} \to k$ be an homomorphism s.t. $h \cdot f = \chi(h) f, \forall h \in \mathfrak{H}$.

Since $\mathfrak{H}$ is free n $\mathfrak{O}$ it exists a prime ideal $\mathfrak{p}$ of $\mathfrak{H}$ contained in the maximal ideal $Ker(\chi)$ and s.t. $\mathfrak{p} \cap \mathfrak{O} = 0$; that's the kernel of an homomorphism $\chi' : \mathfrak{H} \to \mathfrak{O}$, where the reduction mod $\mathfrak{m}$ is χ.

The ideal of $K \otimes \mathfrak{H}$ generated by $\mathfrak{p}$ belongs to the support of the module $K \otimes M$. We can conlude then that there exists a non-zero element f'' of $K \otimes M$ s.t. $hf'' = \chi'(h) f, \forall h \in \mathfrak{H}$. We take then as f' a non-zero multiple of f'' belonging to M. ☐

End of proof of theorem 3.2.2

Considering what we did previously we can suppose that $k \geq 2$ an that f is an eigenvector of T_p, $p \not| Nl$.

As T_l commutes with T_p we can suppose that f is an eigenvector of T_l, $l \not| N$. Then, let

$$\rho_\lambda : G \to GL_2(K_\lambda)$$

to be a representation assosiated with f (see theorem 3.1.1). We can replace ρ_λ by an isomorph representation. Let $\hat{\mathfrak{O}}_\lambda$ be the ring of integers of K_λ. We can suppose that $\rho_\lambda(G) \subset GL_2(\hat{\mathfrak{O}}_\lambda)$ (i.e the completion of $\mathfrak{O}_\lambda$). By reduction mod λ we can deduce from ρ_λ a representation

$$\tilde{\rho}_\lambda : G \to GL_2(k_\lambda).$$

Let ϕ be the semisimplification of $\tilde{\rho}_\lambda$.

ϕ is a semi-simple representation unramified outside Nl which satisfies the formulas from theorem 3.2.2. The group $\phi(G)$ is finite. Due to Čebotarev's density theorem $\phi(G)$ is of the form $F_{\phi,p}$, with $p \not| Nl$.

Considering the definition of k_f, we have that $\forall s \in \phi(G)$ the coefficients of the polynomial $det(1 - sT)$ are in k_f.
The existence of the representation $\rho : G \to GL_2(k_f)$ we are looking for comes from the following lemma.

Lemma 3.2.4. *Let k' be a field and Φ be a group. Let $\phi : \Phi \to Gl_n(k')$ be a semi-simple representation. Let k be a subfield of k' containing the coefficients of the polynomials $det(1 - \phi(s)T), s \in \Phi$. Then ϕ is isomorph to a representation $\rho : \Phi \to Gl_n(k)$.*

Proof. See lemma 6.13 of [DeSe]. □

Chapter 4

Proof of the main theorem

In this chapter we suppose that the considered modular form f is an Eisenstein series or a cusp form.

Before we proceed we state proposition 5.1 from [DeSe] in the case of $k = 1$. This is usefull for the proof of the main theorem.

Proposition 4.0.5. *Let f be a cusp form of type $(1, \epsilon)$ over $\Gamma_0(N)$ not-identically zero. We suppose that f is an eigenfunction of $T_p, p \not| N$ with eigenvalues a_p.*
The series $\sum_{p \not| N} |a_p|^2 p^{-s}$ converges for $s > 1$ real and we have

$$\sum_{p \not| N} |a_p|^2 p^{-s} \leq log(\frac{1}{s-1}) + O(1), \text{ for } s \to 1.$$

Proof. See proposition 5.1 from [DeSe]. □

Proposition 4.0.6. *With the considerations of the previous proposition we have that $\forall \eta > 0$ it exists a set of prime numbers X_η and a finite subset Y_η of $\mathbb{C}$ s.t.*

$$dens.sup X_\eta \leq \eta \text{ and } a_p \in Y_\eta, \forall p \notin X_\eta.$$

Proof. See proposition 5.5 from [DeSe]. □

We will note with $\mathbf{F}_l$ the finite field with l elements.

Lemma 4.0.7. *If f is an Eisenstein series, there exist two characters χ_1 and χ_2 of $(\mathbb{Z}/N\mathbb{Z})^*$ s.t. $\chi_1 \cdot \chi_2 = \epsilon$ and s.t. $a_p = \chi_1(p) + \chi_2(p), \forall p \not| N$.*
We consider the reducible representation

$$\rho = \chi_1 \otimes \chi_2,$$

where χ_i can be viewed as representations of degree 1 of $\text{Gal}(\overline{\mathbb{Q}}, \mathbb{Q})$.

We suppose that f is a cusp form.

(From proposition 2.7 from [DeSe],) a_p and $\epsilon(p)$ belong to the ring of integers of $\mathfrak{O}_K$ of the number field K, that we suppose to be Galois over $\mathbb{Q}$.

Let L be the set of prime numbers l which split completelly in K. For every $l \in L$ we choose a place λ_l of K that extends l. The corresponding residual field is equal to $\mathbf{F}_l$.

Due to theorem 3.2.2, there is a continuous semi-simple representation

$$\rho_l : \mathrm{Gal}\,(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL(\mathbf{F}_l),$$

which is unramified outside Nl and s.t.

$$det(1 - F_{\rho_l,p}T) \equiv 1 - a_pT + \epsilon(p)T^2 \pmod{\lambda_l}, \text{ if } p \not| Nl.$$

Definition 4.0.8. *Let η and M be two positive numbers. We consider the following property for the subgroups G of $GL_2(\mathbf{F}_l)$:*
$C(\eta, M)$: If exists an $H \subset G$ s.t.

$$|H| \geq (1 - \eta)|G|$$

and the set of polynomials $det(1 - hT), h \in H$ has at most M elements.

Proposition 4.0.9. *Let $\eta < \frac{1}{2}$ and $M \geq 0$. It exists a constant $A = A(\eta, M)$ s.t. for every prime number l and for every semisimple group $G \subset GL_2(\mathbf{F}_l)$ satisfying $C(\eta, M)$ we have $|G| \leq A$.*

Proof. Omited. See proposition 7.2 from [DeSe]. □

Let $G_l \subset GL_2(\mathbf{F}_l)$ be the image of ρ_l.

Lemma 4.0.10. *$\forall \eta > 0$ exists a constant M s.t. G_l satisfies the condition $C(\eta, M)$, $\forall l \in L$.*

Proof. From proposition 4.0.6 it exists a subset X_η, of the set P of prime numbers s.t. $dens.supX_\eta \leq \eta$ and s.t. for $p \notin X_\eta$ and that the a_p's for $p \notin X_\eta$ form a finite set.
We note $\mathcal{M}$ the (finite) set of the polynomials $1 - a_pT + \epsilon(p)T^2$, for $p \notin X_\eta$. We note $M = |\mathcal{M}|$.

We claim that G_l satisfies $C(\eta, M)$, $\forall l \in L$.

In deed, let $H_l \subset G_l$ be the set which contains the Frobenius $F_{\rho_l,p}, p \notin X_\eta$ and their conjugates. From Čebotarev's density theorem, we have that $|H_l| \geq (1 - \eta)|G_l|$.

On the other hand, if $h \in H_l$, the polynomial $det(1 - hT)$ is a reduction $\pmod{\lambda_l}$ of an element of $\mathcal{M}$, so it belongs to a set with at most M elements. So, the condition $C(\eta, M)$ is satisfied. □

Lemma 4.0.11. *It exists a constant A s.t. $|G_l| \leq A, \forall l \in L$.*

Proof. Immediate from proposition 4.0.9. ☐

We choose a constant A satisfying 4.0.11. Even by extending K (which makes L smaller), we can suppose that it contains all the n-th roots of unity, for $n \leq A$. Since l splits in K, all n-th roots of unity with $n \leq A$ are in $\mathbf{F}_l$.

Let Y be the set of polynomials $(1-\alpha T)(1-\beta T)$ where α and β are roots of unity with order $\leq A$.

If $p \not| N, \forall l \in L$ it exists $R(T) \in Y$ s.t.

$$1 - a_p T + \epsilon(p) T^2 \equiv R(T) (\text{mod } \lambda_l).$$

As Y is finite, it exists an R s.t. the congruence above is satisfied for infinitelly many l, so then we have the equality

$$1 - a_p T + \epsilon(p) T^2 = R(T),$$

i.e. $1 - a_p T + \epsilon(p) T^2 \in Y$.

Let

$$L' = \{l \in L \mid l > A \text{ and } R, S \in Y, R \neq S \text{ implies } R \not\equiv S \ (\text{mod } \lambda_l)\}.$$

The set $L - L'$ is finite. So L' is infinite. Let $l \in L'$.

The order of the group G_l is prime to l (if not l should divide $|G_l|$ but $|G_l| \leq A < l$).

It results, by a standard argument, that the identity representation $G_l \to GL_2(\mathbf{F}_l)$ is the reduction mod λ_l of a representation $G_l \to GL_2(\mathfrak{O}_{\lambda_l})$, where $\mathfrak{O}_{\lambda_l}$ is the valuation ring of λ_l.
Composing this with the canonical application $G \to G_l$ we obtain a representation

$$\rho : G \to GL_2(\mathfrak{O}_{\lambda_l}).$$

By construction, ρ is unramified outside Nl. If $p \not| Nl$, the eigenvalues of the Frobenius elements $F_{\rho,p}$ are the roots of the unity with order $\leq A$ (because the image of ρ is isomorph to G_l of order $\leq A$) i.e. $det(1 - F_{\rho,p} T) \in Y$.

On the other hand, since the reduction of ρ mod λ_l is ρ_λ, we have

$$det(1 - F_{\rho,p} T) \equiv 1 - a_p T + \epsilon(p) T^2 \ (\text{mod } \lambda_l).$$

But, $det(1 - F_{\rho,p} T), 1 - a_p T + \epsilon(p) T^2 \in Y$ and due to the last relation they are equal i.e.

$$det(1 - F_{\rho,p} T) = 1 - a_p T + \epsilon(p) T^2, \forall p \not| Nl.$$

We replace now l by another prime $l' \in L'$. We obtain a representation $\rho' : G \to GL_2(\mathfrak{O}_{\lambda_{l'}})$ which has the same properties as above for $p \not| Nl'$. In particular

$$det(1 - F_{\rho,p}T) = 1 - a_pT + \epsilon(p)T^2, \forall p \not| Nl'.$$

From Čebotarev's density theorem we have that ρ and ρ' are isomorph over $GL_2(K)$ as representations (consequently and as complex representations i.e. representetions over $GL_2(\mathbb{C})$). It results that ρ is unramified outside N and that

$$det(1 - F_{\rho,p}T) = 1 - a_pT + \epsilon(p)T^2, \forall p \not| N.$$

It remains to show that ρ is irreducible.

We suppose that ρ is not irreducible. Then is the sum of two representations of degree 1, which corrspond to two characters χ_1 and χ_2, unramified outside N, s.t. $\chi_1\chi_2 = \epsilon$ and

$$a_p = \chi_1(p) + \chi_2(p), \forall p \not| N.$$

We then have

$$\sum |a_p|^2 p^{-s} = \sum |\chi_1(p) + \chi_2(p)|^2 p^{-s}.$$

i.e.

$$\sum |a_p|^2 p^{-s} = 2\sum p^{-s} + \sum \chi_1(p)\overline{\chi}_2(p)p^{-s} + \sum \chi_2(p)\overline{\chi}_1(p)p^{-s}.$$

If $s \to 1$, we have that $\sum p^{-s} = \log(\frac{1}{s-1}) + O(1)$.

On the other hand we have that $\chi_1\overline{\chi}_2 \neq 1$ because otherwise we would have $\epsilon = (\chi_1)^2$ and $\epsilon(-1) = 1$. From here it results that

$$\sum \chi_1(p)\overline{\chi}_2(p)p^{-s} = O(1) \text{ and } \sum \chi_2(p)\overline{\chi}_1(p)p^{-s} = O(1).$$

We have

$$\sum |a_p|^2 p^{-s} = 2\log(\frac{1}{s-1}) + O(1) \text{ for } s \to 1$$

That contradicts proposition 4.0.5 and this finishes the proof.