A CONJECTURAL MASS FORMULA FOR MOD P GALOIS REPRESENTATIONS

by

Tommaso Giorgio Centeleghe

A dissertation submitted to the faculty of
The University of Utah
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

Department of Mathematics

The University of Utah

May 2009

THE UNIVERSITY OF UTAH GRADUATE SCHOOL

SUPERVISORY COMMITTEE APPROVAL

of a dissertation submitted by

Tommaso Giorgio Centeleghe

This dissertation has been read by each member of the following supervisory committee and by majority vote has been found to be satisfactory.

	Chair: Gordan Savin
	Chandrashekhar Khare
	Wiesława Nizioł
	Dragan Miličić
	Dan Ciubotaru

THE UNIVERSITY OF UTAH GRADUATE SCHOOL

FINAL READING APPROVAL

To the Graduate Council of the University of Utah:

I have read the dissertation of Tommaso Giorgio Centeleghe in its final form and have found that (1) its format, citations, and bibliographic style are consistent and acceptable; (2) its illustrative materials including figures, tables, and charts are in place; and (3) the final manuscript is satisfactory to the Supervisory Committee and is ready for submission to The Graduate School.

Date	Gordan Savin Chair, Supervisory Committee

Approved for the Major Department

Aaron Betram
Chair/Dean

Approved for the Graduate Council

David S. Chapman
Dean of The Graduate School

ABSTRACT

A recent development in Algebraic Number Theory is Khare and Khare–Winterberger proof of Serre's Modularity Conjecture on two–dimensional mod p representations of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. Using the link between mod p modular forms and mod p Galois representations that this important theorem provides, we formulate a conjectural mass formula for the asymptotics with p of the number of two–dimensional, odd, irreducible mod p Galois representations of $\mathbf{Q}$, of fixed conductor N.

CONTENTS

ACKNOWLEDGMENTS

I would like to express my deep gratitude to professor Chandrashekhar Khare for the invaluable support and constant encouragement that I have received from him in writing this dissertation. Working under his direction was for me a unique experience.

I would like to thank professors Gordan Savin and Wiesława Nizioł for many precious discussions about parts of the material contained in this thesis and about other topics in mathematics. More generally, I want to thank all the members of the Mathematics Department at the University of Utah, staff included, for leaving me with a nice memory of the years spent together.

I want to thank my family members Adina, Armando, Alessandra and Irma. They were able to make me feel close to them, in spite of the physical distance that separated us for most of the last years.

I am grateful to all my Italian friends for not having forgotten me completely. Among them I want to mention Antonio, Francesco and Tobia, who still are the wonderful persons they were in summer '99.

Finally, special thanks go to my friend Gueorgui, who graduated last year from this same department and has always been a unique friend and fellow mathematician.

INTRODUCTION

Between the mid 50s and the end of the 60s, Eichler, Shimura, Deligne and Serre proved a fundamental theorem relating any classical modular form f that is an eigenvectors of the Hecke operators, to a *compatible system* of p-adic Galois representations $\rho_{f,p}$ of $\mathbf{Q}$ (cf. 3.1.1). Each member $\rho_{f,p}$ of the system is a two–dimensional representation of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ with coefficients in a finite extension of $\mathbf{Q}_p$, every $\rho_{f,p}$ is unramified outside $S \cup \{p\}$, where S is a fixed set of primes depending only on f (the level). The compatibility condition is the requirement that for every $\ell \notin S \cup \{p\}$, the *trace* and *determinant* of $\rho_{f,p}(\mathrm{Frob}_\ell)$ are algebraic integers depending only on ℓ (and not on p) that are dictated by the modular form f. Here Frob_ℓ is an element of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ that induces the Frobenius automorphism on a residue field of $\bar{\mathbf{Z}}$ of characteristic ℓ. The fact that $\ell \notin S \cup \{p\}$ implies that the operator $\rho_{f,p}(\mathrm{Frob}_\ell)$ is well defined up to conjugation, and we can therefore speak of its *trace* and *determinant*.

The Galois group $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ is compact and $\rho_{f,p}$ may be reduced mod p

$$\bar{\rho}_{f,p} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$$

to give an odd, semisimple representation. That this construction is a rich source of mod p Galois representations of $\mathbf{Q}$ was clear to Serre, who, in the 70's, formulated (the first version of) his Modularity Conjecture, asserting that in fact *any* odd, irreducible representations of $G_{\mathbf{Q}}$ arises in this way (cf. 3.1.2).

It is a basic but important fact that for any given prime p, if we let the weight of the modular form f vary, keeping its level fixed, then we will only obtain *finitely* many mod p representations $\bar{\rho}_{f,p}$, up to isomorphism. The statement is completely false for the characteristic zero representations $\rho_{f,p}$. A restatement of this fact is that there are only finitely many systems of mod p Hecke eigenvalues arising from modular forms of level N. The study of the algebra of mod p modular forms is the successful attempt, started by Swinnerton-Dyer and Serre, to construct a finite dimensional Hecke module from which all the mod p systems of Hecke eigenvalues arise (cf. 3.2.5): up to a twist by the power

of the mod p cyclotomic character, every $\bar{\rho}$ arising from some form of weight k also arises from a from of weight $k_1 \leq p+1$.

After the proof of Serre's conjecture by Khare and Khare-Winterberger, it is tempting to try and count such number of eigensystems, to answer the question of how many mod p representations $\bar{\rho}$ of the type above are there. This is the guiding problem of our thesis. The difficulties arising in this project are given by the fact that, a part from the reduction to weight $\leq p+1$, there is not a systematic way to predict when two distinct characteristic zero eigensystems collapse into the same one, when reduced mod p. However, it is expected that in the range $(2, \ldots, p+1)$ this phenomenon of congruences "rarely" happens.

We do not get any definite answer towards the solution of this ambitious problem. Instead we would like to present a conjectural formula that should grasp the asymptotic with p of the number of two–dimensional, odd, irreducible, mod p Galois representations of $\mathbf{Q}$, of fixed conductor N.

CHAPTER 1

MODULAR FORMS AND HECKE ALGEBRAS

1.1 Modular forms

1.1.1 Analytic definition

Let N be an integer ≥ 1, consider the morphism of reduction mod N

$$\mathrm{SL}_2(\mathbf{Z}) \to \mathrm{SL}_2(\mathbf{Z}/N).$$

Attached to N there are three subgroups of $\mathrm{SL}_2(\mathbf{Z})$

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

respectively defined as preimages of the three subgroups of $\mathrm{SL}_2(\mathbf{Z}/N)$ given by

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} \subset \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \right\} \subset \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right\}.$$

The group $\Gamma(N)$ is the *principal congruence subgroup* of level N, it is normal in $\mathrm{SL}_2(\mathbf{Z})$ and $\Gamma_1(N)$ is normal in $\Gamma_0(N)$. The morphism of reduction mod N is surjective (cf. [53], §1.6, lemma 1.38), therefore there are the following isomorphisms

$$\begin{gathered} \mathrm{SL}_2(\mathbf{Z})/\Gamma(N) \simeq \mathrm{SL}_2(\mathbf{Z}/N), \\ \Gamma_1(N)/\Gamma(N) \simeq \mathbf{Z}/N, \\ \Gamma_0(N)/\Gamma_1(N) \simeq (\mathbf{Z}/N)^*. \end{gathered}$$

A finite index subgroup Γ of $\mathrm{SL}_2(\mathbf{Z})$ containing $\Gamma(N)$, for some $N \geq 1$, is called a *congruence subgroup*, the smallest integer N so that $\Gamma(N) \subset \Gamma$ is the *level* of Γ.

Let z be any point in the complex upper half plane $\mathbf{H}$, and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$ any element. Set $\gamma\, z = \frac{az+b}{cz+d}$ and define the *factor of automorphy* j by $j(\gamma, z) = (cz + d)$. We have

$$j(\gamma\delta, z) = j(\gamma, \delta\, z) j(\gamma, z), \tag{1.1}$$

for all γ, $\delta \in \mathrm{SL}_2(\mathbf{Z})$ and $z \in \mathbf{H}$.

For any any complex valued function f defined on the upper half plane $\mathbf{H}$, and any fixed integer k, the function $f|[\gamma]_k$ on $\mathbf{H}$ is defined by

$$f|[\gamma]_k(z) = j(\gamma, z)^{-k} f(\gamma z).$$

The cocycle condition 1.1 ensures that the map $(f, \gamma) \to f|[\gamma]_k$ defines a right action of $\mathrm{SL}_2(\mathbf{Z})$ on the space of complex valued functions on $\mathbf{H}$. Continuous (resp. holomorphic) functions are preserved by the action. Observe that $f|[-1_2]_k = (-1)^k f$, where 1_2 is the two by two identity matrix.

Definition 1.1.1. A *modular form* f of weight k on a congruence subgroup Γ is a $\mathbf{C}$–valued function on $\mathbf{H}$ satisfying the following conditions:

i) f is holomorphic on $\mathbf{H}$;

ii) $f|[\gamma]_k = f$, for all $\gamma \in \Gamma$;

iii) f is holomorphic at the cusps of Γ.

The complex vector space of such modular forms is denoted by $\mathbf{M}_k(\Gamma)$

The precise meaning of the last condition is that for any $\sigma \in \mathrm{SL}_2(\mathbf{Z})$ there exists an integer $h > 0$ so that the function $f|[\sigma]_k$ has a series expansion of the form

$$f|[\sigma]_k(z) = \sum_{n \geq 0} a_n e^{2\pi i n z/h}.$$

If the integer $h > 0$ is minimal, then one can show that h divides N if the cusp $\sigma(\infty)$ is *regular* and $2h$ divides N if such cusp is *irregular* (cf. [53]). The power series in the variable $q = e^{2\pi i z/h}$ so obtained for h minimal is the *Fourier series* of f at the cusp $\sigma(\infty)$. It depends only on the Γ–orbit of $\sigma(\infty) \in \mathrm{P}^1(\mathbf{Q})$ and it is denoted by $f_{\sigma(\infty)}$.

Definition 1.1.2. A modular form $f \in \mathbf{M}_k(\Gamma)$ is called a weight k *cusp form* for Γ if the constant terms in all of its Fourier expansions $f_{\sigma(\infty)}$ are zero. The subspace of cusp forms is denoted by $\mathbf{M}_k^0(\Gamma)$.

If Γ contains $\Gamma_1(N)$, then it follows from ii) that $f(z+1) = f(z)$ and the Fourier series f_∞ at the cusp infinity takes the form

$$f_\infty(q) = \sum_{n \geq 0} a_n q^n, \qquad \text{where} \quad q = e^{2\pi i z}. \tag{1.2}$$

We will often identify f with its expansion f_∞.

Remark 1.1.3. In the definition of modular form, condition ii) can be checked only on a set of generators for the group Γ considered. For example if $\Gamma = \mathrm{SL}_2(\mathbf{Z})$ we have that f satisfies ii) if and only if

ii)' $f(z+1) = f(z)$;

ii)" $f(-\frac{1}{z}) = z^k f(z)$;

for all $z \in \mathbf{H}$. This follows from the fact that $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ generate $\mathrm{SL}_2(\mathbf{Z})$. For a more general congruence subgroup Γ, f has to satisfy more functional equations.

Proposition 1.1.4. *For every congruence subgroup Γ, the space $M_k(\Gamma)$ is finite dimensional. Moreover, $\mathbf{M}_0(\Gamma) = \mathbf{C}$ and if $k < 0$ then $\mathbf{M}_k(\Gamma)$ is trivial.*

A proof of the proposition can be found in [53] where dimension formulas for $\mathbf{M}_k(\Gamma)$ and $\mathbf{M}_k^0(\Gamma)$ are given (for $k \neq 1$) in terms of certain integers attached to Γ (cusps, elliptic points, index $[\mathrm{SL}_2(\mathbf{Z})/\langle \pm 1 \rangle : \Gamma\langle \pm 1 \rangle / \langle \pm 1 \rangle]$).

If $f \in \mathbf{M}_k(\Gamma)$ and $g \in \mathbf{M}_j(\Gamma)$, then it follows that $fg \in \mathbf{M}_{k+j}(\Gamma)$ and the space

$$\mathbf{M}(\Gamma) = \bigoplus_{k \geq 0} \mathbf{M}_k(\Gamma)$$

is a graded $\mathbf{C}$–algebra called *algebra of modular forms* for Γ.

We will only be concerned with the congruence subgroup $\Gamma_1(N)$. Since

$$\begin{pmatrix} 1 & 0 \\ 0 & N \end{pmatrix}^{-1} \Gamma_1(N^2) \begin{pmatrix} 1 & 0 \\ 0 & N \end{pmatrix} \subset \Gamma(N),$$

there is no loss of generality in making this reduction, as the theory of modular forms on $\Gamma(N)$ can be essentially deduced from that of $\Gamma_1(N^2)$.

Let now f be a modular form on $\Gamma_1(N)$, and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$. Since the group $\Gamma_1(N)$ is normal in $\Gamma_0(N)$, it follows that the map

$$f \longrightarrow f|[\gamma]_k, \tag{1.3}$$

defines an automorphism of $\mathbf{M}_k(\Gamma_0(N), \epsilon)$ which depends only on the class of γ in $\Gamma_0(N)/\Gamma_1(N)$. It is easy to see that the subspace of cusp forms is preserved by 1.3. In view of the identification

$$\Gamma_0(N)/\Gamma_1(N) \ni \gamma \longrightarrow d \in (\mathbf{Z}/N)^*,$$

we see that the automorphism in 1.3 is determined by the class of d modulo N, we will denote it by $\langle d \rangle$ and call it diamond operator.

If $\epsilon : (\mathbf{Z}/N)^* \to \mathbf{C}^*$ is any Dirichlet character, then, in view of the identification

$$\Gamma_0(N)/\Gamma_1(N) \ni \gamma \to d \in (\mathbf{Z}/N)^*,$$

we can think of ϵ as a character of $\Gamma_0(N)$, trivial on $\Gamma_1(N)$.

Definition 1.1.5. A modular form f of type (k, ϵ) on $\Gamma_0(N)$ is a modular form on $\Gamma_1(N)$ so that $f|[\gamma]_k = \epsilon(d)f$ for any $\gamma \in \Gamma_0(N)$. The space of such modular forms is denoted by $\mathbf{M}_k(\Gamma_0(N), \epsilon)$, the subspace of cusp forms is denoted by $\mathbf{M}_k^0(\Gamma_0(N), \epsilon)$.

Notice that the condition $f|[\gamma]_k = \epsilon(d)f$ for $\gamma = -1_2 \in \Gamma_0(N)$ is $(-1)^k f = \epsilon(-1)f$, therefore the space $\mathbf{M}_k(\Gamma_0(N), \epsilon)$ is nonzero only if ϵ and k have the same parity, that is $\epsilon(-1) = (-1)^k$.

Since the group $\Gamma_0(N)/\Gamma_1(N) \simeq (\mathbf{Z}/N)^*$ is finite, its action on $\mathbf{M}_k(\Gamma_1(N))$ can be made diagonal, we have

Proposition 1.1.6. *The space* $\mathbf{M}_k(\Gamma_1(N))$ *decomposes as direct sum*

$$\mathbf{M}_k(\Gamma_1(N)) = \bigoplus_{\epsilon} \mathbf{M}_k(\Gamma_0(N), \epsilon),$$

where ϵ *ranges through all characters of* $(\mathbf{Z}/N)^*$ *of the same parity of* k.

If $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is an element of $\Gamma_0(N)$ then the automorphism of $\mathbf{M}_k(\Gamma_1(N))$ given by $f \to f|[\gamma]_k$ is called *diamond operator* and denoted by $\langle d \rangle$.

1.1.2 Examples

Let $z \in \mathbf{H}$ be any complex number in the upper half plane. For any even integer $k > 2$, define the k-th Eisenstein series $\tilde{G}_k$ for $\mathrm{SL}_2(\mathbf{Z})$ by

$$\tilde{G}_k(z) = \sum_{(n,m)\neq(0,0)} \frac{1}{(nz+m)^k}.$$

Thank to the assumption $k > 2$, the series converges absolutely and uniformly on every compact subset of $\mathbf{H}$, thus defining a holomorphic function on $\mathbf{H}$ that can be easily verified to satisfy the equation

$$\tilde{G}_k|[\gamma]_k(z) = \tilde{G}_k(z),$$

for all $z \in \mathbf{H}$, $\gamma \in \mathrm{SL}_2(\mathbf{Z})$ (cf. [41], VII, 2.3. Serre denotes by G_{2k} what we call $\tilde{G}_k$).

The constant term of the Fourier series expansion of $\tilde{G}_k$ at infinity involves the values of the Riemann ζ function at the even positive integers, these are related to Bernoulli numbers. In the literature, Bernoulli numbers are defined using different normalizations. For us, the k-th Bernoulli number b_k is the rational number defined by the formal equality between power series of $\mathbf{Q}[[x]]$

$$\frac{x}{e^x - 1} = \sum_{k \geq 0} b_k \frac{x^k}{k!}, \tag{1.4}$$

it is easy to see that $b_k = 0$ for any k odd > 1. We have the formula (cf. [33], X, th. 3.1)

Proposition 1.1.7. *If k is an even integer > 1, then*

$$2\zeta(k) = -\frac{b_k}{k!}(2\pi i)^k.$$

In particular we see that b_k is nonzero for all *even* integers ≥ 2, $b_k > 0$ for $k \equiv 2 \bmod 4$ and $b_k < 0$ for $k \equiv 0 \bmod 4$. The following proposition describes the Fourier expansion of $\tilde{G}_k$.

Proposition 1.1.8. *$\tilde{G}_k(z)$ belongs to $\mathbf{M}_k(SL_2(\mathbf{Z}))$. Its Fourier series expansion is given by*

$$\tilde{G}_k(z) = -\frac{b_k}{k!}(2\pi i)^k + 2\frac{(2\pi i)^k}{(k-1)!}\sum_{n \geq 1} \sigma_{k-1}(n) q^n,$$

where $\sigma_i(n) = \sum_{0<d|n} d^i$.

(cf. Serre, loc. cit., VII, prop. 8. Serre uses a different normalization for the b_k's)

In particular, the constant term of any of the Eisenstein series $\tilde{G}_k$ is not zero and $\tilde{G}_k$ is not cuspidal.

We will be interested in studying congruences mod p between coefficients of different Eisenstein series. It is convenient to set, for k even > 2

$$G_k = \tilde{G}_k \frac{(k-1)!}{2^{k+1}(-1)^{k/2}\pi^k}.$$

We have

$$G_k = -\frac{b_k}{2k} + \sum_{n \geq 1} \sigma_{k-1}(n) q^n, \tag{1.5}$$

which is a power series with *rational* coefficients with bounded denominators. The normalized Eisenstein series of weight k is defined as

$$E_k = -\frac{2k}{b_k} G_k = 1 - \frac{2k}{b_k}\sum_{n \geq 1} \sigma_{k-1}(n) q^n. \tag{1.6}$$

The following is well known (cf. Serre, loc. cit., VII, 3.2).

Proposition 1.1.9. *There is an isomorphism of* $\mathbf{C}$*–algebras* $\mathbf{C}[X,Y] \simeq \mathbf{M}(SL_2(\mathbf{Z}))$*, which sends* X *to* $\tilde{G}_4$ *and* Y *to* $\tilde{G}_6$*. The space of modular forms of weight* k *for* $SL_2(\mathbf{Z})$ *is spanned by the monomials* $\tilde{G_4}^a \tilde{G_6}^b$*, with* $4a + 6b = k$*.*

If follows from the proposition that the smallest weight k for which the space of cusp forms $\mathbf{M}_k^0(\mathrm{SL}_2(\mathbf{Z}))$ is nonzero is $k = 12$, and that such space is one–dimensional.

Definition 1.1.10. The Ramanujan Δ function is the element of $\mathbf{M}_{12}^0(\mathrm{SL}_2(\mathbf{Z}))$ defined by

$$\Delta = \frac{1}{1728}(E_4^2 - E_6^2).$$

The Fourier coefficients of Δ define the celebrated τ function

$$\Delta(q) = \sum_{n \geq 1} \tau(n) q^n.$$

There is the following product expansion for Δ

Theorem 1.1.11. $\Delta = q\Pi_{n\geq 1}(1-q^n)^{24}$

The theorem is due to Jacobi (cf. Serre, loc. cit., VII. th. 6). In particular, this implies that $\tau(n)$ is an integer for all $n \geq 0$, which can also be checked from the definition of Δ in terms of E_4 and E_6.

The Ramanujan τ function satisfies several congruences modulo $2^5, 3^3, 5^2, 7, 23, 691$. More precisely, if p is a prime number then

$$\tau(p) \equiv 1 + p^{11} \pmod{2^5} \text{ if } p \neq 2, \tag{1.7}$$

$$\tau(p) \equiv p^2 + p^9 \pmod{3^3} \text{ if } p \neq 3, \tag{1.8}$$

$$\tau(p) \equiv p + p^{10} \pmod{5^2}, \tag{1.9}$$

$$\tau(p) \equiv p + p^4 \pmod{7}, \tag{1.10}$$

$$\begin{gathered}\tau(p) \equiv 0 \pmod{23} \text{ if } p \text{ is not a quadratic residue mod } 23,\\ \tau(p) \equiv 2 \pmod{23} \text{ if } p \text{ is of the form } x^2 + 23y^2,\\ \tau(p) \equiv -1 \pmod{23} \text{ if } p \text{ is a quadratic residue and it is not of the form } x^2 + 23y^2,\end{gathered} \tag{1.11}$$

$$\tau(p) \equiv 1 + p^{11} \pmod{691}. \tag{1.12}$$

The congruences have been discovered by different mathematicians (cf. [42], [55]), congruence 1.12 is due to Ramanujan himself. Swinnerton-Dyer had obtained improvements of congruences 1.7 to 1.10 (cf. [55]), for simplicity we have not included them here.

1.1.3 Geometric definition

Let S be any scheme. An elliptic curve E over S is a proper, smooth curve

$$\pi : E \to S,$$

enabled with a section $e \in E(S)$, so that all of its geometric fibers E_k are connected curves of genus one. The invertible sheaf $\Omega^1_{E/S}$ on E has degree zero on each fiber and

$$\underline{\omega}_E = \pi_*(\Omega^1_{E/S}), \tag{1.13}$$

is an invertible sheaf on S (cf. [27]). If $S = \mathrm{Spec}(A)$ is the spectrum of a ring, we will say that E is an elliptic curve A.

Proposition 1.1.12. *Let E be an elliptic curve over S, then E inherits a unique structure of commutative S–group scheme that recovers the group structure on the geometric fibers $E \otimes k$, for any geometric point k of S.*

(cf. [27], II, th. 2.1.2.)

If N is an integer ≥ 1, the kernel E_N of multiplication by N is a *finite flat commutative group scheme* of rank N^2 over S. It is étale over S if and only if N is invertible in $\Gamma(S, \mathcal{O}_S)$.

Let μ_N be the group of N–th roots of unity, viewed as group scheme over S. Consider pairs $(E, \alpha)_S$ where

i) E/S is an elliptic curve;

ii) $\alpha : \mu_N \to E_N$ is an *embedding* of S–group schemes.

Let k be an integer ≥ 0 and T be a scheme over $\mathbf{Z}[1/N]$.

Definition 1.1.13. A *holomorphic modular form* f of weight k for $\Gamma_1(N)$ defined over T is a law that, for any T–scheme S, assigns to every pair $(E, \alpha)_S$ as above an element $f(E, \alpha) \in \underline{\omega}_E^{\otimes k}$ so that the following conditions are satisfied

i) f is compatible with S–isomorphisms of pairs $(E, \alpha)_S$;

ii) f commutes with arbitrary base change $S' \to S$ of schemes above T;

iii) f is "holomorphic" at all the cusps $(\mathrm{Tate}(q), \alpha)_{T \otimes \mathbf{Z}((q))}$.

Let us explain what we mean by iii). The Tate curve $\mathcal{T} = \mathrm{Tate}(q)$ is an elliptic curve over the Laurent series ring $\mathbf{Z}((q))$ (it is even a *generalized* elliptic curve over $\mathbf{Z}[[q]]$ in the sense of [10], II) which is equipped with a canonical differential $\omega_{can} \in \underline{\omega}_{\mathcal{T}}$. The object $(\mathrm{Tate}(q), \alpha)_{T \otimes \mathbf{Z}((q))}$ considered in iii) is the Tate curve, viewed over $T \otimes \mathbf{Z}((q))$,

enabled with an embedding $\alpha : \mu_N \to \mathcal{T}_N$ of group schemes over $T \otimes \mathbf{Z}((q))$. Condition iii) imposes to f a regular behavior on *all* such test objects $(\mathcal{T}, \alpha)_{T \otimes \mathbf{Z}((q))}$, called T–cusps, whose local formulation for any f satisfying i) and ii) is the following: if $\mathrm{Spec}(R) \subset T$ is a suitably small affine open subscheme of T, then the element $f_\alpha(q) \in \mathbf{Z}((q)) \otimes R$ defined by the equality

$$f(\mathcal{T}, \alpha)_{R \otimes \mathbf{Z}((q))} = f_\alpha(q) \underline{\omega}^k_{can,R} \tag{1.14}$$

has to belong to $\mathbf{Z}[[q]] \otimes R$, for all α.

If $T = \mathrm{Spec}(R)$ is affine, then the power series $f_\alpha(q) \in R[[q]]$ attached to α is called *Fourier expansion* of f at the cusp α. Moreover, the subscheme $\mathcal{T}_N$ of $\mathcal{T}$ acquires a natural embedding (cf. [10],II)

$$Id_N : \mu_N \to \mathcal{T}_N \tag{1.15}$$

over $\mathbf{Z}((q)) \otimes \mathbf{Z}[1/N]$. The resulting cusp $(\mathcal{T}, Id_N)_{R \otimes \mathbf{Z}((q))}$ is called cusp at infinity, the corresponding Fourier expansion for f is denoted by $f_\infty(q)$. We will be interested only in holomorphic modular forms, and we will refer to them simply as modular forms.

Definition 1.1.14. A modular form f of weight k for $\Gamma_1(N)$ defined over a ring R is called *cusp* form if for all embeddings $\alpha : \mu_N \to \mathcal{T}_N$ the constant term of the expansion f_α is zero.

If R is any ring that is also a $\mathbf{Z}[1/N]$–algebra, then $\mathbf{M}_k(\Gamma_1(N), R)$ denotes the R module of modular forms of weight k for $\Gamma_1(N)$ over R, and $\mathbf{M}^0_k(\Gamma_1(N), R)$ denotes the submodule of cusp forms. We will be concerned only with modular forms on $\Gamma_1(N)$ and the reference to this congruence subgroup will sometimes be dropped, we will write $\mathbf{M}_k(R)$ and $\mathbf{M}^0_k(R)$ for the above spaces.

If $R = \mathbf{C}$, then the space $\mathbf{M}_k(\Gamma_1(N), \mathbf{C})$ just defined coincide with the classical space of modular forms $\mathbf{M}_k(\Gamma_1(N))$ introduced in section 1.1.1, moreover "geometric" cusp forms correspond to "classical" cusp forms. The Fourier expansion $f(q)$ at the cusp 1.15 is the expansion given in formula 1.2 (cf. [10], VII, §4).

It will be useful to interpret the definition of modular forms in terms of the modular curve $X_1(N)$, when it exists.

Proposition 1.1.15. *If $N > 4$ then the functor that assigns to any $\mathbf{Z}[1/N]$–scheme S the set of S–isomorphism classes of pairs $(E, \alpha)_S$, where E is an elliptic curve over S and $\alpha : \mu_N \to E_N$ is an embedding of S–group schemes, is representable by an affine curve*

$X_1^0(N)$ which is smooth and geometrically connected over $\mathbf{Z}[1/N]$, it is finite flat over the j–line $\mathbf{Z}[1/N, j]$ and étale over the open subset where j and $j - 1728$ are invertible. The modular curve $X_1(N)$ is defined to be the normalization of $X_1^0(N)$ over the projective j–line $P^1_{\mathbf{Z}[1/N]}$.

(cf. [27], III, VIII.).

The scheme $X_1(N) - X_1^0(N)$ over $\mathbf{Z}[1/N]$ is a disjoint union of sections that are in natural bijection with pairs $(\mathrm{Tate}(q), \alpha)_{\mathbf{Z}((q))[1/N]}$ as α describes all the embeddings $\alpha_i : \mu_N \to \mathcal{T}_N$, where $\mathcal{T}$ is the Tate curve, viewed over $\mathbf{Z}((q))[1/N]$.

Let N be an integer > 4, the curve $X_1^0(N)$ is equipped with the universal elliptic curve $\mathcal{E}$, and with the invertible sheaf $\underline{\omega}_{\mathcal{E}}$ defined by formula 1.13. The line bundle $\underline{\omega}_{\mathcal{E}}$ extends uniquely to a line bundle on $X_1(N)$ which will be denoted in the same way (cf. [17], §2).

Proposition 1.1.16. *Let R be a ring over $\mathbf{Z}[1/N]$. The space $\mathbf{M}_k(R)$ of modular forms of weight k for $\Gamma_1(N)$ defined over R is equal to $H^0(X_1(N) \otimes R, \underline{\omega}_{\mathcal{E}}^k)$.*

The proposition is a restatement of the definition of modular form together with a calculation on the Tate curve $\mathcal{T}$ (cf. Gross, loc. cit.).

The following important fact will allow us to "lift" modular forms over $\mathbf{Z}/p$ to characteristic zero, in most cases.

Proposition 1.1.17. *For $k \geq 2$, $N > 4$ the natural map*

$$\mathbf{M}_k(\mathbf{Z}[1/N]) \otimes R \to \mathbf{M}_k(R)$$

is an isomorphism. If R is an algebra over $\mathbf{Z}[1/6]$, the same statement holds for $k \geq 2$ and all $N \geq 1$.

The above proposition is proved for $N > 4$ using the existence of the modular curve $X_1(N)$. The vanishing of $H^1(X_1(N), \underline{\omega}_{\mathcal{E}}^k)$ for $k \geq 2$ and the identification of the module $\mathbf{M}_k(R)$ with $H^0(X_1(N) \otimes R, \underline{\omega}_{\mathcal{E}}^k)$ imply the result by a standard base changing argument (cf. [25], §1.7). For $N \leq 4$, the proof can be found in [25], §1.8 and [17], §10.

Concerning modular forms over characteristic zero fields we have the following

Proposition 1.1.18. *Let K be any field of characteristic zero. Then*

$$\mathbf{M}_k^0(\Gamma_1(N), K) = \mathbf{M}_k^0(\Gamma_1(N), \mathbf{Q}) \otimes K,$$

for all $N \geq 1$.

(cf. [10], VII, 3.2.)

In particular, the space of classical modular forms $\mathbf{M}_k^0(\Gamma_1(N), \mathbf{C})$ has a $\mathbf{Q}$–structure. This is clear for $N = 1$, where an explicit basis for $\mathbf{M}_k^0(\Gamma_1(N), \mathbf{C})$ is given by appropriate monomials in the Eisenstein series E_4 and E_6, whose q–expansions have rational coefficients.

The following proposition is known as the *q–expansion principle*.

Proposition 1.1.19. *The map $\mathbf{M}_k(\Gamma_1(N), R) \to R[[q]]$ that sends f to $f(q)$ is an injective morphism of R-modules whose image is contained in $\mathbf{Z}[[q]] \otimes R$.*

The proof of this statement can be adapted from [25] using that $X_1(N)$ is geometrically connected.

1.2 Hecke operators

1.2.1 Hecke operators on q–expansion

Hecke operators are commuting endomorphisms of $\mathbf{M}_k(\Gamma)$ first introduced in the classical setting to prove the multiplicative properties of the Fourier coefficients of the Ramanujan τ function. Using the language of the moduli problem, Hecke operators can be defined naturally on "geometric" modular forms over any ring R.

The classical definition of Hecke operators for $\Gamma_1(N)$ as averaging operators on lattice functions can be found in cf [33]. For the abstract construction of the Hecke ring for any congruence subgroup Γ cf. [53]. The general definition of Hecke operators on the space $\mathbf{M}_k(R)$ for $\Gamma_1(N)$ is carried out in [25]. We will content ourself to the description of the action of the Hecke operators on $\mathbf{M}_k(\Gamma_1(N), R)$ through their effect on the Fourier expansion at infinity, our presentation follows that of [17].

Let $d \in (\mathbf{Z}/N)^*$, S a scheme over $\mathbf{Z}[1/N]$ and $(E, \alpha)_S$ an elliptic curve E over S with an embedding $\alpha : \mu_N \to E_N$. By definition, the pair

$$\langle d \rangle (E, \alpha)_S = (E, d\alpha)_S,$$

is deduced from $(E, \alpha)_S$ by precomposing α with the automorphism of μ_N given by multiplication by d. It follows that $(\mathbf{Z}/N)^*$ acts on $X_1^0(N)$ and the action extends uniquely to an action on the modular curve $X_1(N)$. For any ring R over $\mathrm{Spec}(\mathbf{Z}[1/N])$, the automorphism $\langle d \rangle$ of $X_1(N)$ induces an R-linear automorphism $f \to f|\langle d \rangle$ of the space $\mathbf{M}_k(\Gamma_1(N), R)$ by the formula

$$f|\langle d \rangle (E, \alpha) = f(E, d\alpha).$$

In the case $R = \mathbf{C}$, this coincides with the diamond operator of section 1.1.1.

Definition 1.2.1. If $\epsilon : (\mathbf{Z}/N)^* \to R^*$ is a group homomorphism and $f \in \mathbf{M}_k(\Gamma_1(N), R)$, then we will say that f has type (k, ϵ) if $f|\langle d\rangle = \epsilon(d)f$.

In order for a nonzero form $f \in \mathbf{M}_k(\Gamma_1(N), R)$ to have type (k, ϵ), we must have that $\epsilon(-1) = (-1)^k$.
Let ℓ be a prime not dividing N and $f \in \mathbf{M}_k(R)$ a modular form of weight k for $\Gamma_1(N)$ defined over R. Assume that $k \geq 2$ and let

$$f(q) = \sum_{n\geq 0} a_n q^n,$$

$$f|\langle \ell\rangle(q) = \sum_{n\geq 0} b_n q^n,$$

be the Fourier expansions of f and $f|\langle \ell\rangle$ at infinity. Then the *Hecke operator* T_ℓ defines a modular form $f|T_\ell \in \mathbf{M}_k(R)$ whose Fourier expansion is given by

$$f|T_\ell(q) = \sum_{n\geq 0} a_{n\ell} q^n + \ell^{k-1} \sum_{n\geq 0} b_n q^{n\ell}. \tag{1.16}$$

If r is a prime that divides N, then the analog of T_ℓ is the Hecke operator U_r whose action on $\mathbf{M}_k(R)$, for $k > 1$, is described by

$$f|U_r(q) = \sum_{n\geq 0} a_{nr} q^n. \tag{1.17}$$

The formulas for the Hecke operators T_ℓ and U_r on $\mathbf{M}_1(R)$, for ℓ, r primes with $\ell \nmid N$ and $r|N$, are more delicate, as in this case one cannot conveniently make use of the fact that any modular form $f \in \mathbf{M}_k(R)$ defined over R "lifts" to an element $\tilde{f}$ of $\mathbf{M}_k(\mathbf{Z}[1/N]) \otimes R$ (cf. prop 1.1.17). However, if R contains a subring of $\bar{\mathbf{Q}}$ or R is a field of characteristic p then formulas 1.16 and 1.17 are still valid (cf. [17]) and this will be enough for our purposes.

Proposition 1.2.2. *The endomorphisms T_ℓ, U_r and $\langle d\rangle$, for $l \nmid N$, $r|N$ and $d \in (\mathbf{Z}/N)^*$, of the space $\mathbf{M}_k(R)$ commute with each other and preserve the cuspidal subspace $\mathbf{M}_k^0(R)$.*

Proof. The commutativity of the algebra generated by the operators T_ℓ and U_r follows from a direct computation using formulas 1.16 and 1.17. In order to show that T_ℓ and U_r commute with $\langle d\rangle$ one may use their moduli theoretic definition (cf. [25]). □

Observe that if $f = \sum_{n\geq 0} a_n q^n \in \mathbf{M}_k(\Gamma_1(N), R)$ has type (k, ϵ), and $\ell \nmid N$ then formula 1.16 for T_ℓ becomes

$$f|T_\ell(q) = \sum_{n\geq 0} a_{n\ell} q^n + \epsilon(\ell)\ell^{k-1} \sum_{n\geq 0} a_n q^{n\ell}.$$

A consequence is that if $f = \sum_{n\geq 0} a_n q^n$ is an eigenvector for T_ℓ, with eigenvalue λ_ℓ, then

$\lambda_\ell a_0 = (1 + \epsilon(\ell)\ell^{k-1})a_0$;

$\lambda_\ell a_n = a_{n\ell}$, for all n so that $(\ell, n) = 1$;

$\lambda_\ell a_{n\ell^m} = a_{n\ell^{m+1}} + \epsilon(\ell)\ell^{k-1} a_{\ell^{m-1}}$, for all n, $m \geq 1$.

In particular, if $a_1 = 0$ then $a_{n\ell} = 0$ for all $n > 0$.

Similarly if $f \in \mathbf{M}_k(\Gamma_1(N), R)$ is an eigenvector for the Hecke operator U_r, r prime, $r|N$, with eigenvalue λ_r, then

$\lambda_r a_0 = a_0$;

$\lambda_r a_n = a_{nr}$, for all $n > 0$.

In particular, if $a_1 = 0$ then $a_{nr} = 0$ for all $n > 0$.

Corollary 1.2.3. *Let f be an eigenform for all the Hecke operators T_ℓ, and U_r of type (k, ϵ). If $a_1 = 0$ then the Fourier expansion of f is constant.*

The following corollary gives a description of systems of eigenvalues arising from modular forms with invertible constant term at the expansion at infinity.

Corollary 1.2.4. *Let f be an eigenform for all the Hecke operators T_ℓ, and U_r, of type (k, ϵ). If a_0 is invertible, then $\lambda_\ell = (1 + \epsilon(\ell)\ell^{k-1})$ for $\ell \nmid N$, and $\lambda_r = 1$, for all $r|N$.*

Definition 1.2.5. We say that $f = \sum_{n\geq 0} a_n q^n \in \mathbf{M}_k(\Gamma_1(N), R)$ of type (k, ϵ) is a normalized eigenform if it is an eigenvector for all the Hecke operators T_ℓ and U_r, and satisfies $a_1 = 1$.

If f is a normalized eigenform, then the previous formulas translate into the multiplicative properties of the Fourier coefficients of f that can be stated as follows

Proposition 1.2.6. *$f = \sum_{n\geq 0} a_n q^n \in \mathbf{M}_k(\Gamma_1(N), R)$ be a normalized eigenform of type (k, ϵ). Then for primes ℓ, r with $\ell \nmid N$ and $r|N$, we have*

$$f|T_\ell = a_\ell f \text{ for } \ell \nmid N$$

$$f|U_r = a_r f \text{ for } r|N.$$

Moreover, we have the following formal Euler product

$$\sum_{n\geq 1} a_n n^{-s} = \Pi_{r|N}(1 - a_r r^{-s})^{-1} \Pi_{\ell\nmid N}(1 - a_\ell \ell^{-s} + \epsilon(\ell)\ell^{k-1-2s})^{-1}.$$

In particular, if f is cuspidal and normalized, then it is uniquely determined by its type and by the eigenvalues (a_p), where p ranges through the entire set of prime numbers.

The Ramanujan Δ function is a normalized eigenform of $\mathbf{M}^0_{12}(\mathrm{SL}_2(\mathbf{Z}), \mathbf{Z})$, the Euler product of the proposition gives the multiplicative relations of the τ function

i) $\tau(mn) = \tau(m)\tau(n)$, if $(m, n) = 1$;

ii) $\tau(p^n) = \tau(p)\tau(p^{n-1}) - p^{11}\tau(p^{n-2})$, if p is prime, $n \geq 2$.

1.2.2 Classical Hecke algebras on $\Gamma_1(N)$ and new forms

In this section we specialize to the classical case $R = \mathbf{C}$ and describe the very special features of the Hecke operators in this setting. We explain how the theory of newforms of Atkin–Lehner (cf. [2]) answers the problems arising from the non–semisimplicity of the Hecke algebra. We refer to [33] for more details and for the proofs. The Hecke operator U_r, for a prime r dividing N, will be here denoted by T_r.

Let $N \geq 1$ be an integer and $\epsilon : (\mathbf{Z}/N)^* \to \mathbf{C}^*$ a Dirichlet character. We are going to consider several commutative $\mathbf{C}$–algebras generated by Hecke operators inside the endomorphisms ring of appropriate spaces of modular forms. They all go under the general name of *Hecke algebras*. The notation that we adopt is explained in the table below. The Hecke algebra of the first column is the $\mathbf{C}$–subalgebra of the endomorphisms ring of the space of modular forms of the second column, which is generated by the Hecke operators listed in the third column. In the table, ℓ is any prime number that may divide N, unless otherwise specified, and d is a class in $(\mathbf{Z}/N)^*$.

Hecke algebra	Space of modular forms	Generators
$\mathcal{H}_{k,N}$	$\mathbf{M}_k(\Gamma_1(N))$	T_ℓ, $\langle d\rangle$
$\mathcal{H}^0_{k,N}$	$\mathbf{M}^0_k(\Gamma_1(N))$	T_ℓ, $\langle d\rangle$
$\mathcal{H}^{0,N}_{k,N}$	$\mathbf{M}^0_k(\Gamma_1(N))$	T_ℓ with $\ell \nmid N$, $\langle d\rangle$
$\mathcal{H}_{k,\epsilon}$	$\mathbf{M}_k(\Gamma_0(N), \epsilon)$	T_ℓ
$\mathcal{H}^0_{k,\epsilon}$	$\mathbf{M}^0_k(\Gamma_0(N), \epsilon)$	T_ℓ
$\mathcal{H}^{0,N}_{k,\epsilon}$	$\mathbf{M}^0_k(\Gamma_0(N), \epsilon)$	T_ℓ with $\ell \nmid N$

Let $\mathcal{H}$ be any of the Hecke algebras above, and let $\mathbf{M}(\mathcal{H})$ denote the space of modular forms upon which $\mathcal{H}$ acts. If $t \in \mathcal{H}$ and $f \in \mathbf{M}(\mathcal{H})$, then $f|t$ denotes the image of f with

respect to the endomorphism t. The Hecke algebras appearing with the superscript "0" are those that act on the cuspidal part of the appropriate space of modular forms and are the ones we will be considering most. Even though the Hecke operators T_ℓ acting on $\mathbf{M}(\mathcal{H})$ clearly depend on k and ϵ, we decided, by abuse of notation, to keep only the prime ℓ in the subscript. The commutativity of $\mathcal{H}$ follows from proposition 1.2.2.

Definition 1.2.7. A system of Hecke eigenvalues arising from $\mathbf{M}_k(\Gamma_1(N))$ is a collection of complex numbers $\Phi = (a_\ell)$ index by primes $\ell \nmid N$ so that there exists a nonzero $f \in \mathbf{M}_k(\Gamma_1(N))$ with $f|T_\ell = a_\ell f$, for all $\ell \nmid N$. If f may be taken to be cuspidal then Φ will be said cuspidal. If f may be taken to be of type (k, ϵ), where ϵ is a certain character of $(\mathbf{Z}/N)^*$, then we will say that Φ arises from $\mathbf{M}_k(\Gamma_0(N), \epsilon)$, or that Φ is of type (k, ϵ).

In the definition, the restriction to the collection of eigenvalues a_ℓ, for primes $\ell \nmid N$, may seem innatural. However, there is the following proposition:

Proposition 1.2.8. *Let $f \in \mathbf{M}_k(\Gamma_1(N))$ be a nonzero, common eigenvector of the T_ℓ's, where ℓ is a prime not dividing N, and let $\Phi = (a_\ell)$ be the associated system of eigenvalues. Then there exists $g \in \mathbf{M}_k(\Gamma_1(N))$ which is an eigenvector of the T_ℓ's, for any prime ℓ, and of the diamond operators $\langle d \rangle$, for $d \in (\mathbf{Z}/N)^*$, so that $g|T_\ell = a_\ell g$, for all primes $\ell \nmid N$. Furthermore, g is unique up to multiplication by a nonzero constant.*

Proof. If $k = 0$ the space $\mathbf{M}_k(\Gamma_1(N))$ is one–dimensional and the proposition is trivial. Assume $k > 0$, and let $V(\Phi)$ be the largest subspace of $\mathbf{M}_k(\Gamma_1(N))$ on which T_ℓ acts by multiplication by a_ℓ, for all primes $\ell \nmid N$. By assumption $f \in V(\Phi)$ and $V(\Phi)$ is not trivial. The operators T_ℓ, for a prime $\ell|N$, and $\langle d \rangle$, for $d \in (\mathbf{Z}/N)^*$, commute with each other and commute with all the T_ℓ's, for all primes $\ell \nmid N$. It follows that they preserve $V(\Phi)$ and that they have is a common eigenvector $g \in V(\Phi)$, thus the existence of g follows.

To prove the uniqueness of g we first point out that a consequence of theorem 3.1.1 is that the type of g is uniquely determined by the system of eigenvalues Φ: there exists a unique character ϵ so that $g \in \mathbf{M}_k(\Gamma_0(N), \epsilon)$ (in fact we have that $V(\Phi) \subset \mathbf{M}_k(\Gamma_0(N), \epsilon)$). Let $g = \sum_{n \geq 0} b_n q^n$ be the Fourier expansion of g, we have that $b_1 \neq 0$, for otherwise g would be constant, by corollary 1.2.3, and this would imply $k = 0$ and contradict $k > 0$. Therefore up to re–scaling we can assume that $b_1 = 1$, i.e., that g is a normalized form of type (k, ϵ). From proposition 1.2.6, we see that all the coefficients b_n's of g, for $n \geq 2$,

are uniquely determined, and it is now easy to see that this forces b_0 to be uniquely determined as well. In fact assume that there were a normalized eigenform g' of the same type (k, ϵ) as g, and belonging to the system of eignevalues Φ, then we would have that $g - g'$ is constant which would imply $k = 0$, contradicting $k > 0$. □

The proposition is known as the *multiplicity one* result for the Hecke algebra $\mathcal{H}_{k,N}$. Let us enphasize the following corollary, already mentioned in the proof of the proposition:

Corollary 1.2.9. *Let Φ be a system of Hecke eigenvalues arising from $\mathbf{M}_k(\Gamma_1(N))$. Then Φ arises from $\mathbf{M}_k(\Gamma_0(N), \epsilon)$, for a unique character ϵ.*

Let $f \in \mathbf{M}_k(\Gamma_1(N))$ be a nonzero modular form that is a common eigenvector for all the Hecke operators T_ℓ and $\langle d \rangle$. Attached to f there is a homomorphism of $\mathbf{C}$–algebras

$$\lambda_f : \mathcal{H}_{k,N} \to \mathbf{C},$$

uniquely determined by the formulas $f|T_\ell = \lambda_f(\ell)f$ and $\lambda_f(\langle d \rangle) = \epsilon(d)$. Here ϵ is the character that determines the isotypical component $\mathbf{M}_k(\Gamma_0(N), \epsilon)$ to which f belongs. Notice that λ_f factors through the natural projection $\mathcal{H}_{k,N} \to \mathcal{H}_{k,\epsilon}$. Conversely,

Proposition 1.2.10. *Let $\mathcal{H}$ be any of the Hecke algebras defined above and $\mathbf{M}(\mathcal{H})$ the corresponding space of modular forms. If $\lambda : \mathcal{H} \to \mathbf{C}$ is any abstract homomorphism of $\mathbf{C}$–algebras, then there exists a nonzero $f \in \mathbf{M}(\mathcal{H})$ so that*

$$f|t = \lambda(t)f,$$

for all $t \in \mathcal{H}$.

Proof. The proposition follows from lemma 4.2.2, section 4.2.1. □

If $f \in \mathbf{M}_k(\Gamma_0(N), \epsilon)$ is a normalized eigenform, the system (a_l) of Hecke eigenvalues to which f belongs is of great arithmetical interest, as will be evident in chapter three. The semisimplicity of $\mathcal{H}_{k,\epsilon}$ is therefore a natural matter to investigate. As it turns out, $\mathcal{H}_{k,\epsilon}$ is *not* semisimple, in general. The theory of newforms explains to what extent this semisimplicity fails to hold for the action of $\mathcal{H}^0_{k,\epsilon}$ on the space of cusp forms for $\Gamma_1(N)$.

Concerning the noncuspidal system of eigenvalues, we have already seen that systems attached to noncuspidal forms $f = \sum_{n \geq 0} a_n q^n$ so that $a_0 \neq 0$ are classified (cf. corollary 1.2.4). The following proposition, due to Hecke, describes the eigensystems coming from more general noncuspidal eigenforms.

Proposition 1.2.11. *Let $f \in \mathbf{M}_k(\Gamma_0(N), \epsilon)$ be a noncuspidal form which is an eigenvector for all the Hecke operators T_ℓ, with $\ell \nmid N$, with associated eigenvalue λ_ℓ. Then, there exists characters ϵ_1, ϵ_2 of $(\mathbf{Z}/N)^*$ with $\epsilon = \epsilon_1\epsilon_2$ so that*

$$\lambda_\ell = \epsilon_1(\ell) + \epsilon_2(\ell)\ell^{k-1},$$

for all $\ell \nmid N$. Moreover, for all pairs ϵ_1, ϵ_2 of characters of $(\mathbf{Z}/N)^*$ so that $\epsilon_1\epsilon_2(-1) = (-1)^k$ there exists a noncuspidal form $f \in \mathbf{M}_k(\Gamma_0(N), \epsilon_1\epsilon_2)$ belonging to the system of eigenvalues (λ_ℓ), where $\lambda_\ell = \epsilon_1(\ell) + \epsilon_2(\ell)\ell^{k-1}$.

The proof may be found in [12], where Eisenstein series for $\Gamma_1(N)$ are explicitely constructed, cf. also [38].

For the rest of this section we will investigate the spectrum of the cuspidal Hecke algebra $\mathcal{H}^0_{k,\epsilon}$ alone, acting on $\mathbf{M}^0_k(\Gamma_1(N))$.

The space $\mathbf{M}^0_k(\Gamma_0(N), \epsilon)$ inherits a positive hermitian form called *Petersson inner product* (cf. [33], p. 37). If $f, g \in \mathbf{M}^0_k(\Gamma_0(N), \epsilon)$, then their inner product will be denoted by $< f, g >$, where, again, we drop any reference to the space $\mathbf{M}_k(\Gamma_0(N), \epsilon)$ considered. A computation carried out in ([33] p.112) shows that

Proposition 1.2.12. *Let ℓ be a prime, with $\ell \nmid N$. Then $< f|T_\ell, g >= \epsilon(\ell) < f, g|T_\ell >$ for any $f, g \in \mathbf{M}^0_k(\Gamma_0(N), \epsilon)$. In particular, T_ℓ commutes with its adjoint and the action of T_ℓ on $\mathbf{M}^0_k(\Gamma_0(N), \epsilon)$ can be made diagonal.*

Let $\Phi^i = (\lambda^{(i)}_\ell)$ describe the systems of Hecke eigenvalues appearing in the space $\mathbf{M}^0_k(\Gamma_1(N))$, where $1 \leq i \leq r$. Also, let ϵ_i be the character of $(\mathbf{Z}/N)^*$ corresponding to Φ_i (cf. corollary 1.2.9). We have

Corollary 1.2.13. *The Hecke algebra $\mathcal{H}^{0,N}_{k,N}$ is semisimple. The morphism*

$$\lambda : \mathcal{H}^{0,N}_{k,N} \to \mathbf{C}^r$$

which sends T_ℓ to $(\lambda^{(1)}_\ell, \ldots, \lambda^{(r)}_\ell)$ and $\langle d \rangle$ to $(\epsilon_1(d), \ldots, \epsilon_r(d))$ is an isomorphism.

The corollary explains the conveniency in considering only Hecke operators T_ℓ for ℓ prime to N. However, the algebra $\mathcal{H}^{0,N}_{k,N}$ does not act on $\mathbf{M}^0_k(\Gamma_1(N))$ with multeplicity one. Meaning that if (a_ℓ) is the set of eigenvalues of T_ℓ, $\ell \nmid N$, associated to a common eigenvector $f \in \mathbf{M}^0_k(\Gamma_0(N), \epsilon)$ with character ϵ, then the eigenspace corresponding to this system of eigenvalues has dimension greater than one, in general. What it is true is that

the eigenspace attached to a system of eigenvalues (a_ℓ) and character ϵ is one–dimensional if and only if the form is *new*, in a sense that we make now precise.

Before treating new forms we define what *old forms* are. Let M, d be positive integers so that M divides N with $M < N$ and d divides M/N. Let ϵ be a character of $(\mathbf{Z}/N)^*$ that factors through the natural map $(\mathbf{Z}/N)^* \to (\mathbf{Z}/M)^*$. Then

Proposition 1.2.14. *There is a map $\pi(M,d) : \mathbf{M}_k^0(\Gamma_1(M),\epsilon) \to \mathbf{M}_k^0(\Gamma_1(N),\epsilon)$ that intertwines the action of all the Hecke operators T_ℓ for ℓ not dividing N. The effect of $\pi(d)$ on q–expansion at infinity is given by*

$$\pi(M,d)(f(q)) = d^k f(q^d),$$

in particular $\pi(M,1)$ is the natural inclusion of $\mathbf{M}_k^0(\Gamma_1(M),\epsilon)$ in $\mathbf{M}_k^0(\Gamma_1(N),\epsilon)$.

For the proof of the proposition cf. [33], VIII.

Definition 1.2.15. The space of *old cusp forms* $\mathbf{M}_k^{0,-}(\Gamma_0(N),\epsilon)$ is defined to be the sum of all the subspaces of $\mathbf{M}_k^0(\Gamma_0(N),\epsilon)$ images of $\pi(M,d)$ for all M, d as above.

The space of *cuspidal new forms* is defined as follows

Definition 1.2.16. The space of cuspidal new forms $\mathbf{M}_k^{0,+}(\Gamma_0(N),\epsilon)$ is the orthogonal complement of $\mathbf{M}_k^{0,-}(\Gamma_0(N),\epsilon)$ in $\mathbf{M}_k^0(\Gamma_0(N),\epsilon)$ with respect to the Petersson inner product.

We further set $\mathbf{M}_k^{0,+}(\Gamma_1(N))$ be the direct sum of $\mathbf{M}_k^{0,+}(\Gamma_0(N),\epsilon)$, as ϵ runs through the characters of $(\mathbf{Z}/N)^*$.

The following is a multeplicity one result for the space of new forms and constitutes the main theorem in the Atkin–Lehner theory. The proof may be found in [33], VIII. The original paper of Atkin–Lehner (cf. [2]) treated only the case of modular forms with trivial character.

Theorem 1.2.17. *The space $\mathbf{M}_k^{0,+}(\Gamma_1(N),\epsilon)$ is precisely the direct sum of all the common eigenspaces for $\mathcal{H}_{k,\epsilon}^{0,N}$ that are one–dimensional.*

1.2.3 Integral properties of Hecke algebras

Let N be an integer ≥ 1 and $\mathbf{M}_k^0(\Gamma_1(N),\mathbf{C}) = \mathbf{M}_k^0(\mathbf{C})$ be the space of modular forms of weight k for $\Gamma_1(N)$ defined over $\mathbf{C}$. The following proposition is [11], prop. 2.7:

Proposition 1.2.18. *Let L be the set of $f \in \mathbf{M}_k^0(\mathbf{C})$ so that $(f|\langle d\rangle)_\infty \in \mathbf{Z}[[q]]$, for all $d \in (\mathbf{Z}/N)^*$. Then*

i) L is a finite free $\mathbf{Z}$–module stable by the all operators T_ℓ and $\langle d\rangle$;

ii) for any field K of characteristic zero we have $\mathbf{M}_k^0(\Gamma_1(N), K) = K \otimes L$;

iii) for any prime ℓ the eigenvalues of T_ℓ acting on $\mathbf{M}_k^0(\mathbf{C})$ are algebraic integers;

iv) for any normalized, cuspidal eigenform $f = \sum_{n\geq 1} a_n q^n \in \mathbf{M}_k^0(\mathbf{C})$ the system of eigenvalues $(a_\ell) \in \mathbf{C}$ lies in a finite extension of $\mathbf{Q}$;

v) for f as in iv), we have that for every automorphism σ of $\mathbf{C}$, the cusp form $\sigma(f)$ is so that $\sigma(f)|T_\ell = \sigma(a_\ell)\sigma(f)$, if f is of type (k, ϵ) then $\sigma(f)$ is if type $(k, \sigma(\epsilon))$.

Proof. If $f \in \mathbf{M}_k^0(\mathbf{Q})$ then $\langle f\rangle \in \mathbf{M}_k^0(\mathbf{Q})$ for all $d \in (\mathbf{Z}/N)^*$ and its expansion $(\langle f\rangle)_\infty(q) \in \mathbf{Z}[[q]] \otimes \mathbf{Q}$ has bounded denominators. It follows that a multiple of f lies in L and $\mathbf{Q} \otimes L = \mathbf{M}_k^0(\mathbf{Q})$. Now, by proposition 1.1.18 we have $K \otimes L = \mathbf{M}_k^0(K)$ for all fields of characteristic zero. The fact that L is a finite $\mathbf{Z}$–module is a direct consequence of the finite dimensionality of $\mathbf{M}_k^0(\mathbf{C}) = \mathbf{C} \otimes L$, that L is stable by the operators T_ℓ (resp. $\langle d\rangle$) follows directly from the explicit formulas 1.16 and 1.17 (resp. is obvious). The monic characteristic polynomial of any of the T_ℓ's has integer coefficients and hence its roots are algebraic integers, i), ii) and iii) are proved. Observe that normalized, cuspidal eigenforms f are in bijection, we know, with $\mathbf{C}$–algebras homomorphism λ_f from $\mathcal{H}_{k,\epsilon}^0$ to $\mathbf{C}$. The eigenvalues $a_\ell = \lambda_f(T_\ell)$ and $\epsilon(d) = \lambda_f(\langle d\rangle)$ are algebraic integers and the algebra $\mathcal{H}_{k,\epsilon}^0$ is finite over $\mathbf{C}$. This readily implies iv). Part v) follows immediately from the fact that $\mathbf{M}_k^0(\mathbf{C}) = \mathbf{M}_k^0(\mathbf{Q}) \otimes \mathbf{C}$. Alternatively, to obtain homomorphism $\lambda_{\sigma(f)}$, we might have considered the composition $\sigma \circ \lambda_f$ and applied proposition 1.2.10 to show that $\sigma(f)$ is a normalized, cuspidal eigenform. □

Part iii) of the proposition could have been proved classically, without using proposition 1.1.18 (cf. [53], th. 3.5.2 for $k > 1$ and [11], 2.8 for the case $k = 1$).

Denote now by $\mathcal{H}_{k,N}^{0,N}(\mathbf{Z})$ the *subring* of the $\mathbf{C}$–algebra $\mathcal{H}_{k,N}^{0,N}$ generated over $\mathbf{Z}$ by the Hecke operators T_ℓ, with $\ell \nmid N$, and by the diamond operators $\langle d\rangle$, for $d \in (\mathbf{Z}/N)^*$. The structure of the ring $\mathcal{H}_{k,N}^{0,N}(\mathbf{Z})$ is given by

Proposition 1.2.19. *The ring $\mathcal{H}_{k,N}^{0,N}(\mathbf{Z})$ embeds as a finite index subring in a finite product $\prod_i \mathcal{O}_i$, where $\mathcal{O}_i$ is the ring of integers of a suitable number field K_i.*

Proof. The proof in a somewhat more abstract setting is given in proposition 4.2.6, section 4.2.2. □

1.2.4 Systems of Hecke eigenvalues mod p

In this section we collect basic results on the nature of systems of Hecke eigenvalues mod p. These facts are general and they depend only on the integral structure of $\mathbf{M}_k^0(\mathbf{C})$ preserved by the Hecke operators (cf prop. 1.2.18). The proofs of all the statements of this section are given in section 4.2.3, where a suitable axiomatic setting is developed.

Let p be a prime and $N > 0$ an integer prime to p. Consider the family of Hecke operators T_ℓ, for a prime $\ell \nmid N$, and $\langle d \rangle$, for $d \in (\mathbf{Z}/N)^*$, acting on $\mathbf{M}_k(\Gamma_1(N), \mathbf{F}_p)$. Assume that $f \in \mathbf{M}_k(\Gamma_1(N), \mathbf{F}_p) \otimes \overline{\mathbf{F}}_p$ is a form of type (k, ϵ), for some $\epsilon : (\mathbf{Z}/N)^* \to \overline{\mathbf{F}}_p^*$, which is a common eigenvector for all the Hecke operators T_ℓ's. Let a_ℓ be the eigenvalue of T_ℓ to which f belongs.

Definition 1.2.20. The collection of eigenvalues $\Phi = (a_\ell)$ for the Hecke operators T_ℓ, indexed by primes $\ell \nmid N$, is called a mod p system of Hecke eigenvalues arising from the space $\mathbf{M}_k(\Gamma_1(N), \mathbf{F}_p)$. If a form f giving rise to Φ may be taken in the cuspidal subspace $\mathbf{M}_k^0(\Gamma_1(N), \mathbf{F}_p) \otimes \overline{\mathbf{F}}_p$, then Φ will be called a cuspidal system.

The definition of system of Hecke eigenvalues adopted is consistent with the definition used in Chapter 4, section 4.2.1, where $K = \mathbf{F}_p$, the space V is $\mathbf{M}_k(\Gamma_1(N), \mathbf{F}_p)$ and the commuting family of operators is given by the Hecke operators T_ℓ, for a prime $\ell \nmid N$, and $\langle d \rangle$, for $d \in (\mathbf{Z}/N)^*$.

If $k > 1$ then the map $\mathbf{M}_k^0(\Gamma_1(N), \mathbf{Z}[1/N]) \otimes \mathbf{F}_p \to \mathbf{M}_k^0(\Gamma_1(N), \mathbf{F}_p)$ is surjective and the algebra of endomorphisms of $\mathbf{M}_k(\Gamma_1(N), \mathbf{F}_p)$ generated by the Hecke operators T_ℓ, for a prime $\ell \nmid N$, and $\langle d \rangle$, for $d \in (\mathbf{Z}/N)^*$, is $\mathcal{H}_{k,N}^{0,N}(\mathbf{Z}) \otimes \mathbf{F}_p$ where $\mathcal{H}_{k,N}^{0,N}(\mathbf{Z})$ is the ring introduced at the end of section 1.2.3. As proposition 4.2.8 explains, we have

Proposition 1.2.21. *For $k > 1$ the set of mod p systems of Hecke eigenvalues arising from the space $\mathbf{M}_k^0(\Gamma_1(N), \overline{\mathbf{F}}_p)$ is in bijection with the $\overline{\mathbf{F}}_p$–points of the ring $\mathcal{H}_{k,N}^{0,N}(\mathbf{Z})$.*

Remark 1.2.22. The characterization of mod p systems of eigenvalues given in the proposition makes it clear that any characteristic zero system of eigenvalues may be reduced mod p. More precisely, let $\mathfrak{p}$ a prime of $\bar{\mathbf{Z}}$ of resdidual characteristic p, and fix an isomorphism $\bar{\mathbf{Z}} \simeq \overline{\mathbf{F}}_p$. Let $\Phi = (a_\ell)$ be a system of Hecke eigenvalues arising from the space $\mathbf{M}_k^0(\Gamma_1(N), \mathbf{C})$, and let $\lambda : \mathcal{H}_{k,N}^{0,N}(\mathbf{Z}) \to \bar{\mathbf{Z}}$ be the associated ring homomorphism (cf. section 1.2.2). The reduction of λ mod $\mathfrak{p}$ gives a $\overline{\mathbf{F}}_p$–point of $\mathcal{H}_{k,N}^{0,N}(\mathbf{Z})$, which corresponds to a mod p system of eigenvalues.

The following is a special case of proposition 4.2.9.

Proposition 1.2.23. *Let $\Phi = (a_\ell)$ be a cuspidal system of Hecke eigenvalues mod p arising from $\mathbf{M}_k^0(\Gamma_1(N), \mathbf{F}_p)$. Then there exists a system $\tilde{\Phi} = (\tilde{a}_\ell)$ of characteristic zero Hecke eigenvalues arising from $\mathbf{M}_k^0(\Gamma_1(N), \mathbf{Q})$ and a prime $\mathfrak{p}$ of $\bar{\mathbf{Z}}$ of residual characteristic p so that $\tilde{a}_\ell$ mod $\mathfrak{p} = a_\ell$.*

An alternative proof of the statement can be found in [11], lemme 6.11.

We now focus on the mod p systems of eigenvalues arising from the space of new forms $\mathbf{M}_{k,N}^{0,+}(\Gamma_1(N), \epsilon)$ and introduce some notation.

Definition 1.2.24. The subring of $\mathrm{End}_{\mathbf{C}}(\mathbf{M}_{k,N}^{0,+}(\Gamma_1(N)))$ generated by all the Hecke operators T_ℓ and $\langle d \rangle$, for all primes $\ell \nmid N$ and $d \in (\mathbf{Z}/N)^*$, is denoted by $\mathcal{H}_{k,N}^{0,+}(\mathbf{Z})$.

By definition, the $\bar{\mathbf{Z}}$–points of $\mathcal{H}_{k,N}^{0,+}(\mathbf{Z})$ correspond to new forms in $\mathbf{M}_{k,N}^{0,+}(\Gamma_1(N))$ and the dimension $d_{k,N}^+$ of $\mathbf{M}_{k,N}^{0,+}(\Gamma_1(N))$, over the complex numbers, coincides with the rank of $\mathcal{H}_{k,N}^{0,+}(\mathbf{Z})$ as $\mathbf{Z}$–module, by theorem 1.2.17 and proposition 1.2.19 (cf. also the proof of proposition 4.2.6).

Let us denote the set of mod p systems of Hecke eigenvalues arising from $\mathbf{M}_{k,N}^{0,+}(\Gamma_1(N))$ by $E_{k,N}^{0,+}(p)$, it is identified with the set of distinct characteristic p points of $\mathcal{H}_{k,N}^{0,+}(\mathbf{Z})$.

Proposition 1.2.25. *The number $|E_{k,N}^{0,+}(p)|$ is less or equal than $d_{k,N}^+$. Equality holds if and only if the ring $\mathcal{H}_{k,N}^{0,+}(\mathbf{Z}) \otimes \mathbf{F}_p$ is semisimple, that is, $\mathcal{H}_{k,N}^{0,+}(\mathbf{Z}) \otimes \overline{\mathbf{F}}_p \simeq \overline{\mathbf{F}}_p^d$, where $d = d_{k,N}^+$ is the dimension of $\mathcal{H}_{k,N}^{0,+}(\mathbf{Z}) \otimes \mathbf{F}_p$ over $\mathbf{F}_p$.*

Proof. This is corollary 4.2.10 □

We will see that for p and N fixed, the number $|E_{k,N}^{0,+}(p)|$ is *bounded* and, on the other hand, the dimension $d_{k,N}^{0,+}$ *is not*, as the integer k grows indefinitely. In particular, the mod p Hecke algebra $\mathcal{H}_{k,N}^0(\mathbf{Z}) \otimes \mathbf{F}_p$ cannot be expected to be semisimple, as it has been known for long time (cf. [23], [24]). However, it is expected that $\mathcal{H}_{k,N}^{0,+}(\mathbf{Z}) \otimes \mathbf{F}_p$ is semisimple if the weight k is less than or equal to $p+1$.

We end the section rephrasing the semisimplicity condition of $\mathcal{H}_{k,N}^{0,+}(\mathbf{Z}) \otimes \mathbf{F}_p$ in terms of *congruences* between distinct, characteristic zero, cuspidal systems of Hecke eigenvalues.

Proposition 1.2.26. *The following are equivalent*

i) there exist a pair (f, g) of distinct new forms in $\mathbf{M}_{k,N}^{0,+}(\Gamma_1(N), \mathbf{C})$ so that f and g give rise to the same mod p systems of Hecke eigenvalues;

ii) $\mathcal{H}^{0,+}_{k,N}(\mathbf{Z}) \otimes \mathbf{F}_p$ *is not semisimple;*

iii) p *divides the discriminant* $\delta_{k,N}$ *of the ring* $\mathcal{H}^{0,+}_{k,N}(\mathbf{Z})$.

In i) it is implicit that a prime $\mathfrak{p}$ of $\bar{\mathbf{Z}}$ of residual characteristic p has been chosen in order to make sense of the reduction mod p of a system of eigenvalues arising from $\mathbf{M}^{0,+}_{k,N}(\Gamma_1(N), \mathbf{C})$.

For the definition and the properties of the discriminant we refer to section 4.2.4. In that same chapter we obtain a refinement of the proposition which might be of some computational interest and upon which our computations are are based (cf. section 4.2.5).

CHAPTER 2

MODULAR FORMS AND REPRESENTATIONS OF GL_2

2.1 The adelic GL_2 over Q

2.1.1 Basic notions

Let $G = G_{\mathbf{Q}}$ be the algebraic group GL_2, viewed over the ground field $\mathbf{Q}$. If p is a prime of $\mathbf{Q}$, finite or infinite, then G_p denotes $\mathrm{GL}_2(\mathbf{Q}_p)$ and, for p finite, K_p is its maximal compact subgroup $\mathrm{GL}_2(\mathbf{Z}_p)$. The connected component of G_∞ containing the identity is denoted by G_∞^0, the maximal compact subgroup of G_∞ given by the orthogonal group is K_∞, and its connected component containing the identity is K_∞^0. The coordinate θ will be used to parametrize K_∞^0, so that

$$u(\theta) = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}.$$

The adèle ring of $\mathbf{Q}$ is denoted by $\mathbf{A}$, the subring of *finite* adèles is defined by those adèles whose archimedean component is zero, it is denoted by $\mathbf{A}^f$. We have

$$\mathbf{A} = \mathbf{R} \times \mathbf{A}^f.$$

The group $G_{\mathbf{A}} = \mathrm{GL}_2(\mathbf{A})$ is by definition the restricted product of all the G_p's with respect to K_p, we have

$$G_{\mathbf{A}} = G_\infty \times G_{\mathbf{A}^f},$$

where $G_{\mathbf{A}^f}$ is $\mathrm{GL}_2(\mathbf{A}^f)$. For every p, the group $G_{\mathbf{Q}}$ embeds in G_p and it is identified with a subgroup of $G_{\mathbf{A}}$, which is *discrete*. All the G_p's and K_p's, for p finite or infinte, will be thought of as subgroups of $G_{\mathbf{A}}$ when needed, K^f will denote the product of all the K_p's, with p a finite prime.

For any finite prime p, let now K'_p be a subgroup of K_p which is equal to K_p for almost all p and so that, for all p, K'_p surjects onto $\mathbf{Z}_p^*$ under the determinant map. Consider the product

$$K' = \prod_{p<\infty} K'_p,$$

the "Strong Approximation Theorem" for SL_2 over $\mathbf{Q}$ implies that

$$G_{\mathbf{A}} = G_{\mathbf{Q}} G_\infty^0 K'.$$

In particular, if N is any integer ≥ 1, the theorem applies to the family

$$K'_p = K_p(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in K_p | c \equiv 0 \mod N \right\},$$

their product K' will be denoted by $K(N)$.

The group $\mathbf{A}^*$ of units of $\mathbf{A}$ can be regarded inside $\mathbf{A}^2$ thank to the map

$$\mathbf{A}^* \ni a \to (a, a^{-1}) \in \mathbf{A}^2.$$

With the induced subspace topology, $\mathbf{A}^*$ is isomorphic to the product of all the $\mathbf{Q}_p^*$, restricted to the compact group of units $\mathbf{Z}_p^*$, when p is finite. $\mathbf{A}^*$ is the the *idèle* group of $\mathbf{Q}$. The fact that $\mathbf{Q}$ has class number one implies that there is a natural isomorphism between the idèle group $\mathbf{A}^*$ and the direct product of the following closed subgroups

$$\mathbf{A}^* = \mathbf{Q}^* \times \mathbf{R}_{>0}^* \times \hat{\mathbf{Z}}^*,$$

where $\hat{\mathbf{Z}}^* = \prod_p \mathbf{Z}_p^*$ is the unit group of $\mathbf{A}^f$, $\mathbf{R}_{>0}^*$ consists of the connected component of $\mathbf{R}^*$ containig the identity, and $\mathbf{Q}^*$ is diagonally embedded in $\mathbf{A}^*$. The idèle group $\mathbf{A}^*$ is isomorphic to the center $Z_{\mathbf{A}}$ of $G_{\mathbf{A}}$, there is a decomposition

$$Z_{\mathbf{A}} = \mathbf{Q}^* \times Z_{G_\infty}^0 \times Z_{\mathbf{A}^f} \tag{2.1}$$

that recovers that of $\mathbf{A}^*$ above. Here $Z_{G_\infty}^0$ is the connected component of the center of G_∞ containing the identity and $Z_{\mathbf{A}^f}$ is the center of $G_{\mathbf{A}^f}$.

A *grossencharacter* ω is by definition a continuous quasicharacter

$$\omega : \mathbf{A}^* \to \mathbf{C}^*$$

which is *trivial* on $\mathbf{Q}^*$. It can be viewed as a quasicharacter of $Z_{\mathbf{A}}$, trivial on $Z_{\mathbf{Q}}$.

Let $N \geq 1$ be any integer and let ϵ be a character of $(\mathbf{Z}/N)^*$. We recall how ϵ can be viewed as a character of K^N and of $Z_{\mathbf{A}}$. The ring homomorphism

$$\hat{\mathbf{Z}} \to \hat{\mathbf{Z}}/N = \mathbf{Z}/N$$

induces surjective group homomorphisms

$$\mathrm{GL}_1(\hat{\mathbf{Z}}) = \hat{\mathbf{Z}}^* \to \mathrm{GL}_1(\mathbf{Z}/N) = (\mathbf{Z}/N)^*, \tag{2.2}$$

$$\mathrm{GL}_2(\hat{\mathbf{Z}}) = K^f \to \mathrm{GL}_2(\mathbf{Z}/N). \tag{2.3}$$

The decomposition 2.1 gives a projection map

$$Z_{\mathbf{A}} \to Z_{\mathbf{A}^f} = \hat{\mathbf{Z}}^*,$$

which, composed with the reduction modulo N of 2.2, allow us to identify ϵ with a finite order character of $Z_{\mathbf{A}}$, denoted by ψ_ϵ, which is trivial on $\mathbf{Q}^*$ and on $\mathbf{R}^*_{>0}$. Consider now the reduction map 2.3, and notice that $K(N)$ is the preimage of the subgroup of upper triangular matrices. The surjective map

$$K(N) \ni \begin{pmatrix} a & b \\ c & d \end{pmatrix} \to a \pmod{N} \in (\mathbf{Z}/N)^*,$$

will be used to identify ϵ with a character of $K(N)$, also denoted by ψ_ϵ.

The two procedures define the same character on $Z_{\mathbf{A}} \cap K(N) = \hat{\mathbf{Z}}^*$, and we may therefore view ψ_ϵ as a character of the group $Z_{\mathbf{A}}K(N)$. If p is a finite prime not dividing N and

$$a_p = (1, 1, \ldots, p, \ldots, 1)$$

denotes the idèle whose component at every place different from p is equal to 1, and whose component at the p–th place is p, then observe that we have

$$\epsilon(p) = \psi_\epsilon(a_p)^{-1},$$

where the idéle $a_p \in \mathbf{A}^*$ is viewed as an element of $Z_{\mathbf{A}}$.

2.1.2 Cuspidal representations of $\mathbf{GL}_2(\mathbf{A})$

The groups $G_{\mathbf{A}}$ and its closed subgroup $G_{\mathbf{Q}}Z_{\mathbf{A}}$ are unimodular and the space $G_{\mathbf{Q}}Z_{\mathbf{A}}\backslash G_{\mathbf{A}}$ inherits a right invariant measure. Let ψ be a unitary grossencharacter

$$\psi : Z_{\mathbf{Q}}\backslash Z_{\mathbf{A}} \to \mathbf{C}^*,$$

and consider the space $L^2(\psi)$ of functions Φ on $G_{\mathbf{Q}}\backslash G_{\mathbf{A}}$ such that $\Phi(zg) = \psi(z)\Phi(g)$ for all $z \in Z_{\mathbf{A}}$, $g \in G_{\mathbf{A}}$ and

$$\int_{G_{\mathbf{Q}}Z_{\mathbf{A}}\backslash G_{\mathbf{A}}} |\Phi(g)|^2 dg < \infty.$$

The unitary representation of $G_{\mathbf{A}}$ by right translation on the Hilbert space $L^2(\psi)$ is denoted by ρ_ψ. If U is the standard unipotent subgroup of G, then the *cuspidal* subspace $L^2_0(\psi)$ is defined by the vanishing of the following integral, defined for almost all g,

$$\int_{U_{\mathbf{Q}}\backslash U_{\mathbf{A}}} \Phi(ng)dn,$$

where dn is a measure on $\mathbf{A}$ invariant by translation. The restriction of ρ_ψ to the closed subspace $L^2_0(\psi)$ is denoted by $\rho_{0,\psi}$. A fundamental theorem of Gelfand and Piatetski–Shapiro states that $L^2_0(\psi)$ is completely reducible:

Theorem 2.1.1. *The representation $\rho_{0,\psi}$ decomposes as direct sum*

$$\rho_{0,\psi} = \oplus_\pi m(\pi)\pi,$$

where $m(\pi)$ are positive integers and π ranges through a countable set of unitary, irreducible, representations of $G_{\mathbf{A}}$ that are pairwise nonisomorphic.

The irreducible constituents of $\rho_{0,\psi}$ are called *cuspidal representations*. A result due to Jacquet and Langlands asserts that

Theorem 2.1.2. *The multiplicity $m(\pi)$ of an irreducible constituent of $\rho_{0,\psi}$ is one.*

In the case where $\psi = \psi_\epsilon$ is associated to a Dirichlet character ϵ mod N (cf. 2.1.1), then we shall see in next section how any classical, cuspidal, new eigenform $f \in \mathbf{M}^0_k(\Gamma_0(N), \epsilon)$ corresponds to certain cuspidal representation.

2.1.3 Adelic interpretation of classical modular forms

In this section we fix integers N and k, with $N \geq 1$, and a character ϵ of $(\mathbf{Z}/N)^*$ of the same parity of k, that is $\epsilon(-1) = (-1)^k$. Let ψ_ϵ be the corresponding character of $Z_{\mathbf{A}}K(N)$ defined in section 2.1.1. We would like to consider complex valued functions

$$\Phi : G_{\mathbf{A}} \to \mathbf{C}$$

so that for all $a \in G_{\mathbf{A}}$ we have

i) $\Phi(\gamma a) = \Phi(a)$, for all $\gamma \in G_{\mathbf{Q}}$;

ii) $\Phi(a \cdot u(\theta)) = \Phi(a)e^{i\theta k}$, for all $u(\theta) \in K_\infty^0$;

iii) $\Phi(azu) = \psi_\epsilon(zu)\Phi(a)$, for all $z \in Z_{\mathbf{A}}$, $u \in K(N)$.

Recall that $u(\theta) = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$, and observe that the condition of k and ϵ having the same parity is necessary for a non–zero function Φ satisfying the above conditions to exist, since $k_\infty(\pi) = -1_2 \in Z_{\mathbf{R}} \subset Z_{\mathbf{A}}$.

Notice that a function Φ that in addition to i), ii) and iii) satisfies

$$\int_{G_{\mathbf{Q}}Z_{\mathbf{A}}\backslash G_{\mathbf{A}}} |\Phi(g)|^2 dg < \infty,$$

is nothing else but an element of $L^2(\psi_\epsilon)$ that has a prescribed behavior under the right translation action of the compact open subgroup $K_\infty^0 K(N)$ of $G_{\mathbf{A}}$. The study of functions satisfying the above conditions can therefore be interpreted as the attempt to identify "distinguished" elements in the space $L^2(\psi_\epsilon)$. In what follows our exposition is inspired by that of [58].

If a function Φ as above were to exist then, by the "Strong Approximation Theorem", condition i) implies that that Φ would be uniquely determined on the open subgroup

$$\Omega(N) = G_\infty^0 K(N).$$

On the other hand, it is easy to see that any function Φ' on $\Omega(N)$ that satisfies ii) and iii) for any $a \in \Omega_N$, $z \in Z_{\mathbf{A}} \cap \Omega(N)$ and $u \in K(N)$, extends to a function Φ on $G_{\mathbf{A}}$ that satisfies i), ii) and iii) if and only if

$$\Phi'(\gamma a) = \Phi'(a) \tag{2.4}$$

for all $\gamma \in G_{\mathbf{Q}} \cap \Omega(N)$, this group being the discrete classical $\Gamma_0(N)$.

Let then Φ' be a function on $\Omega(N)$ satisfying ii) and iii). More precisely, this is to say that

$$\Phi'(a \cdot z \cdot u \cdot u(\theta)) = \psi_\epsilon(zu)\Phi'(a)e^{i\theta k}, \tag{2.5}$$

for all $a \in \Omega(N)$, $z \in Z_{\mathbf{A}} \cap \Omega(N)$, $u \in K(N)$ and $\theta \in [0, 2\pi]$.

Clearly Φ' is uniquely determined by its restriction to the archimedean component G^0_∞. Viceversa, a function

$$\Phi'' : G^0_\infty \to \mathbf{C}$$

extends to a function Φ' defined on $\Omega(N)$ and satisfying 2.5, if and only if

$$\Phi''(z_\infty \cdot g_\infty \cdot u(\theta)) = \mathrm{sign}(z_\infty)^k \Phi''(g_\infty) e^{i\theta k}, \tag{2.6}$$

for all $g_\infty \in G^0_\infty$, $z_\infty \in Z_{\mathbf{R}} \simeq \mathbf{R}^*$ and $\theta \in [0, 2\pi]$.

Therefore the original problem of constructing a function $\Phi : G_{\mathbf{A}} \to \mathbf{C}$ satisfying conditions i), ii) and iii), for a given pair (ϵ, k) with $\epsilon(-1) = (-1)^k$, is reduced to that of constructing a function $\Phi'' : G^0_\infty \to \mathbf{C}$ satisfying 2.6 and so that the unique extension $\Phi' : \Omega(N) \to \mathbf{C}$ satisfies

$$\Phi'(\gamma a) = \Phi'(a),$$

for all $\gamma \in G_{\mathbf{Q}} \cap \Omega(N) = \Gamma_0(N)$. In terms of Φ'' this means precisely that

$$\Phi''(\gamma_\infty \cdot g_\infty) = \psi_\epsilon(\gamma_f)^{-1} \Phi''(g_\infty), \tag{2.7}$$

for all $\gamma = \gamma_\infty \gamma_f \in G_{\mathbf{Q}} \cap \Omega(N)$, and all $g_\infty \in G^0_\infty$, where $\gamma_\infty \in G^0_\infty$ is the component at infinity of γ, and $\gamma_f \in K(N)$ is its finite component. Observe that $\psi(\gamma_f)^{-1} = \epsilon(\gamma)$, where ϵ is regarded as a character of $\Gamma_0(N)$ using the normalization of section 1.1.1 (which we recall it was $\epsilon(\gamma) = \epsilon(d)$). Condition 2.7 may therefore be stated as

$$\Phi''(\gamma_\infty \cdot g_\infty) = \epsilon(\gamma_f) \Phi''(g_\infty).$$

Assuming that a function Φ'' satisfying 2.6 is given, we are going to explore what condition 2.7 means. To this end, let $g_\infty = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G^0_\infty$ be any element. We have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \dfrac{ad-bc}{c^2+d^2} & \dfrac{ac+bd}{c^2+d^2} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} d & -c \\ c & d \end{pmatrix}.$$

Set $x = \dfrac{ad-bc}{c^2+d^2}$ and $y = \dfrac{ac+bd}{c^2+d^2}$, and observe that $g_\infty(i) = xi + y$. It follows that

$$\Phi''(g_\infty) = \Phi'' \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \cdot (ci+d)^{-k} (c^2+d^2)^{k/2},$$

equivalently

$$\Phi(g_\infty) = \Phi \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \cdot x^{-k/2} j(g_\infty, i)^{-k}, \tag{2.8}$$

where

$$j(g_\infty, z) = (cz+d)(ad-bc)^{-1/2}$$

is the factor of automorphy.

Let now $\gamma \in G_{\mathbf{Q}} \cap \Omega(N) = \Gamma_0(N)$, by 2.8 the left hand side of 2.7 is

$$\Phi''(\gamma_\infty g_\infty) = \Phi'' \begin{pmatrix} x' & y' \\ 0 & 1 \end{pmatrix} \cdot x'^{-k/2} \cdot j(\gamma_\infty g_\infty, i)^{-k}$$

where x' and y' are so that $x'i + y' = \gamma_\infty(g_\infty(i)) = \gamma_\infty(xi + y)$. Therefore 2.7 becomes

$$\Phi'' \begin{pmatrix} x' & y' \\ 0 & 1 \end{pmatrix} \cdot x'^{-k/2} \cdot j(\gamma_\infty g_\infty, i)^{-k} = \epsilon(\gamma)\Phi'' \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \cdot x^{-k/2} \cdot j(g_\infty, i)^{-k},$$

for all $\gamma \in \Gamma_0(N)$ and $g_\infty \in G^0_\infty$. Since $j(\gamma_\infty g_\infty, i) = j(\gamma_\infty, g_\infty(i)) \cdot j(g_\infty, i)$ we have

$$\Phi'' \begin{pmatrix} x' & y' \\ 0 & 1 \end{pmatrix} \cdot x'^{-k/2} = \epsilon(\gamma)\Phi'' \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \cdot x^{-k/2} \cdot j(\gamma_\infty, g_\infty(i))^k,$$

which is to say that the function f on the upper half plane defined by

$$f(xi + y) = \Phi \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \cdot x^{-k/2}$$

has to satisfy

$$f(\gamma(\tau)) = \epsilon(\gamma) f(\tau) j(\gamma, \tau)^k, \text{ for all } \gamma \in \Gamma_0(N),$$

which is precisely the transformation property of a modular form in $\mathbf{M}_k(\Gamma_0(N), \epsilon)$. We summarize this fact in the next proposition. Let B' be the subgroup of G^0_∞ given by

$$B' = \left\{ g \in G^0_\infty | g = \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \right\}.$$

Proposition 2.1.3. *Let f be a complex valued function defined on the upper half plane $\mathbf{H}$, and let k be any integer. Let $\epsilon : (\mathbf{Z}/N)^* \to \mathbf{C}^*$ be a Dirichlet character of the same parity as k. Define $\phi_f : B' \to \mathbf{C}$ by*

$$\phi_f \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} = f(xi + y)x^{k/2}.$$

Then there exist a function $\Phi_f : G_{\mathbf{A}} \to \mathbf{C}$, extending ϕ_f and satisfying conditions i), ii) and iii) from the beginning of the section, if and only if f satisfies

$$f(\gamma(\tau)) = \epsilon(\gamma) f(\tau) j(\gamma, \tau)^k, \tag{2.9}$$

for all $\gamma \in \Gamma_0(N)$, $\tau \in \mathbf{H}$. If that is the case, then the extension Φ_f is unique, and it is defined by

$$\Phi_f(\gamma g_\infty u) = \psi_\epsilon(u) f(g_\infty(i)) j(g_\infty, i)^{-k}, \tag{2.10}$$

where $\gamma \in G_{\mathbf{Q}}$, $g_\infty \in G^0_\infty$ and $u \in K(N)$. Moreover, any function on $G_{\mathbf{A}}$ satisfying i), ii), iii) arises in this way.

In particular, modular forms provide examples of function satisfying 2.9.

Proposition 2.1.4. *Let $f \in \mathbf{M}_k(\Gamma_0(N), \epsilon)$ be a classical, cuspidal form of type (k, ϵ). Let Φ_f be the complex valued function on $G_{\mathbf{A}}$ defined by 2.10. Then $\Phi_f \in L^2_0(\psi_\epsilon)$.*

Proof. We are only left with showing that the cuspidality of f implies that $|\Phi_f|$ is square integrable on $G_{\mathbf{Q}}Z_{\mathbf{A}}\backslash G_{\mathbf{A}}$ and that Φ_f is cuspidal. We omit this calculation and refer to [39]. □

Now that we have established a natural way to associate to any cuspidal form $f \in \mathbf{M}_k(\Gamma_0(N), \epsilon)$ a function $\Phi_f \in L^2_0(\psi_\epsilon)$, we would like to obtain some representation theoretic information on the $G_{\mathbf{A}}$ submodule generated by Φ_f in $L^2_0(\psi_\epsilon)$. It turns out that if f is a normalized cuspidal eigenform, then Φ_f lies in a unique irreducible constituent π_f of $L^2_0(\psi_\epsilon)$ that can be characterized in terms of f.

In order achieve this goal, we will describe how any cuspidal representation π of $G_{\mathbf{A}}$ decomposes as a "tensor product" of unitary representations π_p of the local groups G_p, uniquely characterized by π. We have not yet explained how to attach to the global representation π the collection of local representations π_p of the groups G_p, but let us anticipate that there is a transparent correspondence

$$f \longleftrightarrow \pi_f$$

between normalized cuspidal *newforms* $f \in \mathbf{M}_k^{0,+}(\Gamma_0(N), \epsilon)$ and cuspidal representations π appearing in $L^2_0(\psi_\epsilon)$ so that

i) the local representation π_∞ of G_∞ is the *discrete series* of lowest weight $k-1$;

ii) the local representations π_p, for p finite and $p \nmid N$, is *unramified*;

iii) the *conductor* of π is N.

The meaning of *discrete series* representation, *unramified* representation and conductor will be explained in sections 2.2.3 and 2.2.4. In the next sections we recall the representation theory of the local groups G_p, introducing the notions needed to understand the dictionary between cuspidal newforms and cuspidal representations of $G_{\mathbf{A}}$ that we have just mentioned.

2.2 Representations of $\mathbf{GL}_2(\mathbf{Q}_p)$

The representation theoretic interpretation of classical modular forms can be formulated in terms of *unitary* representations of $G_{\mathbf{A}}$ and G_p; however, we find it convenient

to recall first the basic theory of the more general class of *admissible* representations for the local groups.

2.2.1 Admissible representations

The definition of admissible representation in the archimedean case is (cf. [8]):

Definition 2.2.1. An admissible representation of G_∞ is a complex vector space V with

i) a linear representation $\pi_K : K_\infty \to \mathrm{GL}_{\mathbf{C}}(V)$, isomorphic to a direct sum of irreducible representations, each one appearing with finite multiplicity;

ii) an action π of the Lie algebra $gl_2(\mathbf{R})$ of $\mathrm{GL}_2(\mathbf{R})$ on V extending the action of $\mathrm{Lie}(K_\infty)$ induced by π_K, and so that for all $k \in K_\infty$ and $X \in gl_2(\mathbf{R})$ we have

$$\pi_K(k)\pi(X)\pi_K(k)^{-1} = \pi(ad(k).X),$$

where $ad(k)$ is the adjoint action of k on $gl_2(\mathbf{R})$.

In the nonarchimedean case the definition is the following:

Definition 2.2.2. For a finite prime p, an admissible representation of G_p is a linear representation

$$\pi : G_p \to \mathrm{GL}_{\mathbf{C}}(V)$$

on a complex vector space V, so that

i) the stabilizer of $v \in V$ is open in G_p, for all v;

ii) for any open subgroup $H \subset G_p$, the subspace V^H of H–invariant elements is finite dimensional.

It follows from i) that the definition is not sensitive to any topology on the space $\mathrm{GL}_{\mathbf{C}}(V)$. Therefore we could replace the field $\mathbf{C}$ with any algebraically closed field of characteristic zero without essentially affecting the definition.

Let p be a prime of $\mathbf{Q}$, finite or infinite, and let B_p be the subgroup of G_p given by upper triangular matrices. The commutator subgroup of B_p is the standard subgroup of unipotent matrices, any quasicharacter of B_p is of the form

$$B_p \ni b = \begin{pmatrix} x_1 & y \\ 0 & x_2 \end{pmatrix} \to \chi_1(x_1)\chi_2(x_2) \in \mathbf{C}^*,$$

for a unique pair (χ_1, χ_2) of quasicharacters of $\mathbf{Q}_p^*$.

Fix a quasicharacter $\chi \sim (\chi_1, \chi_2)$ of B_p, and let $B(\chi_1, \chi_2)$ be the space of smooth functions

$$f : G_p \to \mathbf{C}$$

such that

$$f(bg) = \chi(b)|x_1/x_2|^{1/2} f(g),$$

for all $b \in B_p$, $g \in G_p$, where $|x| = |x|_p$ is the standard absolute value for $p = \infty$ and it is normalized by $|p|_p = 1/p$ for p finite. For p finite, by *smooth* function on G_p we mean a *locally constant*, complex valued function. Denote by $\pi(\chi) = \pi(\chi_1, \chi_2)$ the representation of G_p on the space $B_{K_p}(\chi_1, \chi_2)$ of K_p–finite vectors.

Proposition 2.2.3. *The representation $\pi(\chi) = \pi(\chi_1, \chi_2)$ is admissible. It is irreducible in all cases but in the following:*

$(p = \infty)$ $(\chi_1 \cdot \chi_2^{-1})(t) = t^n sign(t)$, for a nonzero integer n;

$(p < \infty)$ $(\chi_1 \cdot \chi_2^{-1})(t) = |t|$ or $|t|^{-1}$.

If $\pi(\chi_1, \chi_2)$ is irreducible then $\pi(\chi_1, \chi_2) \simeq \pi(\chi_1', \chi_2')$ if and only if $(\chi_1, \chi_2) = (\chi_1', \chi_2')$ or $(\chi_1, \chi_2) = (\chi_2', \chi_1')$.

Proof. For the proof of the proposition cf. [16]. □

The representation $\pi(\chi)$, when irreducible, is said to belong to the *principal series*. In the next proposition we assume that $p = \infty$ and that the pair (χ_1, χ_2) is such that

$$(\chi_1 \cdot \chi_2^{-1})(t) = t^n sign(t), \quad \text{for } n > 0. \tag{2.11}$$

Proposition 2.2.4. *The representation $\pi(\chi_1, \chi_2)$ has a unique, proper, invariant subspace $\sigma(\chi_1, \chi_2)$ that is of finite codimension. The lowest weight for K_∞ in $\sigma(\chi_1, \chi_2)$ is $n + 1$. The representation $\sigma(\chi_1, \chi_2)$ is not isomorphic to any of the principal series representations $\pi(\chi_1', \chi_2')$.*

Proof. For the proof of the proposition cf. Gelbart, loc. cit. □

In the statement of the proposition, *lowest weight* means the smallest positive integer h so that the character of K_∞^0 given by

$$u(\theta) \to e^{i\theta h}$$

occurs in $\sigma(\chi_1, \chi_2)$. The infinite dimensional representation $\sigma(\chi_1, \chi_2)$ is said to belong to the *discrete series*.

Keeping the assumption 2.11 on the pair (χ_1, χ_2), we have that the picture for $\pi(\chi_2, \chi_1)$ is reversed: the representation $\pi(\chi_2, \chi_1)$ has a unique, proper, invariant subspace that is finite dimensional and it is isomorphic to $\pi(\chi_1, \chi_2)/\sigma(\chi_1, \chi_2)$. Moreover the quotient of $\pi(\chi_2, \chi_1)$ by its invariant, proper, subspace is isomorphic to the discrete series $\sigma(\chi_1, \chi_2)$ (cf. Gelbart, loc. cit. for more details) .

Theorem 2.2.5. *Every infinite dimensional, irreducible, admissible representation of $GL_2(\mathbf{R})$ is isomorphic to either a principal series representation $\pi(\chi_1, \chi_2)$ or to a discrete series $\sigma(\chi_1, \chi_2)$.*

Proof. For the proof of the theorem cf. Gelbart, loc. cit. □

Let now p be a finite prime, the decomposition of $\pi(\chi_1, \chi_2)$ is similar to that of the archimedean case: if $(\chi_1 \cdot \chi_2^{-1})(t) = |t|$ then $\pi(\chi_1, \chi_1|.|^{-1})$ contains exactly one irreducible subspace of codimension one giving rise to a *special representation*, denoted by $St(\chi_1, \chi_1|.|^{-1})$, whereas $\pi(\chi_1|.|^{-1}, \chi_1)$ contains exactly one irreducible subspace of dimension one, the quotient is isomorphic to $St(\chi_1, \chi_1|.|^{-1})$.

In the nonarchimedean case there are admissible representations that are not taken in account by the principal series and the special representations. These representations are called *supercuspidal* and they are characterized by the property that their matrix coefficients are compactly supported, modulo the center (cf. [8]). Their parameterization is explained by the local Langlands correspondence which asserts that there is a natural bijection between the isomorphism classes of supercuspidal representations of G_p and two–dimensional, irreducible, complex representations of the Weil group W_p of $\mathbf{Q}_p$ (cf. [8], [39]).

2.2.2 Unitary representations

It is a basic fact recall that any unitary, irreducible representation of G_p is admissible. More precisely,

Theorem 2.2.6. *Let π be an irreducible, unitary representation of G_p on a Hilbert H. Then the underlying representation π^f on the space of K_p–finite vectors is admissible.*

We make the following definition:

Definition 2.2.7. An irreducible, admissible representation π of G_p is said unitarizable if there exists a unitary representation of G_p whose underlying representation on the space of K_p–finite vectors is isomorphic to π.

Let p be the infinite prime, consider two characters χ_i of $\mathbf{R}^*$ as before and write them as $\chi_i = |t|^{s_i} sign(t)^{m_i}$, with $s_i \in \mathbf{C}$ and $m_i = 0$ or 1.

Theorem 2.2.8. *The irreducible, admissible, unitarizable representations of G_∞ are*

i) $\pi(\chi_1, \chi_2)$ with χ_i's both unitary, that is s_1, s_2 are both purely imaginary complex numbers;

ii) $\pi(\chi_1, \chi_2)$ with $s_1 + s_2$ purely imaginary and $s_1 - s_2$ a nonzero real number with $|s_1 - s_2| \leq 1$;

iii) $\sigma(\chi_1, \chi_2)$ with unitary central character $\chi_1\chi_2$.

If p is a finite prime we have

Theorem 2.2.9. *The irreducible, admissible, unitarizable representations of G_p are*

i) $\pi(\chi_1, \chi_2)$ with χ_i's both unitary;

ii) $\pi(\chi_1, \chi_2)$ with $\chi_2 = \bar{\chi}_1^{-1}$ and $(\chi_1\chi_2^{-1})(t) = |t|^r$, with $0 < r < 1$;

iii) $St(\chi_1, \chi_2)$ with unitary central character $\chi_1\chi_2$;

iv) the supercuspidal representations with unitary central character.

In both cases, p finite or infinite, unitarizable representations of type ii) in the theorems are said to belong to the *complementary series* representations. The proofs of the theorems above may be found in [4].

2.2.3 The discrete series of $\mathbf{GL}_2(\mathbf{R})$

Let $k \geq 1$ be an integer, following [8] we define a certain admissible, unitarizable representation D_{k-1} of G_∞ (the representation D_{k-1} defined in [8] is actually non–unitarizable: it is the twist by the central character $\lambda \to \text{sign}(\lambda) \cdot \lambda^k$ of what it is denoted here by D_{k-1}). In order to describe the action of $gl_2(\mathbf{R})$ on D_{k-1}, it is convenient to consider the complexified Lie algebra $gl_2(\mathbf{R}) \otimes \mathbf{C}$, where we pick the basis

$$H = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad X = \frac{1}{2}\begin{pmatrix} 1 & i \\ i & -1 \end{pmatrix}, \quad Y = \frac{1}{2}\begin{pmatrix} 1 & -i \\ -i & -1 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

D_{k-1} has then a basis e_n over $\mathbf{C}$ indexed by the integers $n \equiv k \pmod 2$ so that $|n| \geq k$.

The actions of $gl_2(\mathbf{R}) \otimes \mathbf{C}$ and K_∞ on D_{k-1} satisfy

i) $u(\theta) \cdot e_n = e^{i\theta n} e_n$, for $\theta \in [0, 2\pi]$;

ii) $s \cdot e_n = e_{-n}$, where $s = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \in K_\infty - K_\infty^0$;

iii) $H \cdot e_n = n e_n$, which follows from i);

iv) $X \cdot e_n = \frac{k+n}{2} e_{n+2}$, (0 for $n = -k$);

v) $Y \cdot e_n = \frac{k-n}{2} e_{n-2}$, (0 for $n = k$);

vi) $Z \cdot e_n = 0$.

The Casimir operator is the second order operator $\Omega = \frac{1}{4}(H^2 + 2XY + 2YX)$, it is a central element of the enveloping algebra of $gl_2(\mathbf{R})$. Its eigenvalue on the $gl_2(\mathbf{R})$-module of D_{k-1} is $\lambda = \frac{k}{2}(1 - \frac{k}{2})$ (cf. [4], §2.5).

Let now χ_1, χ_2 the quasi-characters of $\mathbf{R}^*$ defined by

$$\chi_1(t) = \operatorname{sign}(t)^k |t|^{(k-1)/2}, \quad \chi_2(t) = |t|^{-(k-1)/2}.$$

Proposition 2.2.10. *The admissible representation D_{k-1} is isomorphic to the discrete series representation $\sigma(\chi_1, \chi_2)$ for $k > 1$ and to $\pi(\chi_1, \chi_2)$ for $k = 1$.*

Proof. For the proof cf. [16], §4. □

The lowest weight vector $e_k \in D_{k-1}$ characterizes uniquely D_{k-1} among the irreducible unitary representations of G_∞. More precisely,

Proposition 2.2.11. *Let π be an irreducible, admissible, unitarizable representation of G_∞ on the vector space V. Assume that there exists a nonzero $v \in V$ so that*

i) $\pi_K(u(\theta))v = e^{i\theta k} v$, for $\theta \in [0, 2\pi]$;

ii) $\pi(Y) \cdot v = 0$.

Then π is isomorphic to D_{k-1}

Proof. For the proof cf. [39] and the references therein. □

Let now π be an irreducible, admissible, unitarizable representation of G_∞ admitting a realization on a vector space V of smooth complex valued functions on G_∞. Assume

that there exists $\phi \in V$ so that $\phi(z \cdot g \cdot u(\theta)) = e^{ik\theta}\phi(g)$, for all $g \in G_\infty$, $t \in R^*$, $\theta \in [0, 2\pi]$. Then the restriction of ϕ to G^0_∞ satisfies

$$\phi\left(\begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix}\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} u(\theta)\right) = y^{k/2} f(x+iy)e^{ik\theta},$$

for all $t, y > 0$, where $f = f(x+iy)$ is a function on the upper half plane $\mathbf{H}$. In this case the action of the Lie algebra $gl_2(\mathbf{R})$ on V can be made explicit and a direct computation (cf. [39]) shows that

$$Y \cdot \phi = -iy^{1+k/2} e^{i(k-2)\theta} \frac{\partial}{\partial \bar{z}} f(x+iy). \tag{2.12}$$

In particular if $\phi \in V$ as above exists and may be chosen so that $f = f(z)$ is a holomorphic function on the upper half plane, then π is isomorphic to the discrete series D_{k-1}.

2.2.4 Ramification of representations of $\mathbf{GL}_2(\mathbf{Q}_p)$, for $p < \infty$

Let p be any prime number and $\omega : \mathbf{Q}_p^* \to \mathbf{C}^*$ a quasi–character of $\mathbf{Q}_p^*$. We recall that ω is *unramified* if it is trivial on the unit group $\mathbf{Z}_p^*$ or, equivalently, if ω factors through the p–adic norm $|\ |_p : \mathbf{Q}_p^* \to \mathbf{R}^*_{>0}$. In this case ω is uniquely determined by the nonzero complex number $\omega(p)$.

Definition 2.2.12. An admissible, irreducible, infinite dimensional representation π of G_p is called *unramified* if the representation space for K_p has a nonzero fixed vector.

Unramified representations of G_p are also called *spherical* or said to be *class one*.

Proposition 2.2.13. *Let χ_1 and χ_2 be unramified characters of $\mathbf{Q}_p^*$ so that $\chi_1 \cdot \chi_2^{-1} \neq |\ |_p^{\pm 1}$. Then the admissibile, irreducible representation $\pi(\chi_1, \chi_2)$ is class one and the space of K_p–fixed vectors of $\pi(\chi_1, \chi_2)$ is one–dimensional. Furthermore, every admissible, irreducible representation π of G_p that is class one arises in this way.*

This is Th. 4.23 in [16].

Let $\pi = \pi(\chi_1, \chi_2)$ as in the proposition and let $g \in G_p$ be any element. According to the Iwasawa decomposition, g may be written as

$$g = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} k, \tag{2.13}$$

for some $a, b, d \in \mathbf{Q}_p$, with $ad \neq 0$, and $k \in K_p$. Consider the function $f_0 : G_p \to \mathbf{C}$ defined by

$$f_0(g) = |a/d|^{1/2} \chi_1^{\nu_p(a)}(p) \chi_2^{\nu_p(d)}(p).$$

Because χ_1 and χ_2 are unramified, one sees easily that f_0 is well defined, meaning that the definition of f_0 does not depend on the decomposition 2.13 chosen for g. Moreover, it is immediate to verify that f_0 belongs to the space of K_p–fixed vectors of $\pi(\chi_1, \chi_2)$.

If π is not class one, then there is the following theorem of Casselman (cf. [16], [8]):

Theorem 2.2.14. *Let π be any irreducible, admissible representation of G_p on an infinite dimensional space V, with central character ψ. Then there exists a largest ideal $c(\pi) = (p^n)$ of $\mathbf{Z}_p$ such that the space of vectors $v \in V$ so that*

$$\pi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) \cdot v = \psi(a)v,$$

for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in K_p$ with $c \equiv 0$ mod $c(\pi)$, is not empty. Furthermore, this space is one–dimensional.

The ideal $c(\pi) \subset \mathbf{Z}_p$, generated by a power of p, is called the *conductor* of π. Any nonzero vector v satisfying the property in the theorem is called a *new vector* of π.

2.2.5 Hecke operators

Let p be a finite prime, and dg a Haar measure on G_p, normalized in such a way that $\mathrm{vol}(K_p) = 1$. Let $C_c^\infty(G_p)$ be the convolution algebra of smooth, compactly supported, complex valued functions f on G_p. A function ϕ on G_p belongs to $C_c^\infty(G_p)$ if and only ϕ is compactly supported and there exists an open, compact subgroup K of G_p so that ϕ is bi–invariant under K, that is $\phi(ugu') = \phi(g)$ for all $u, u' \in K$, $g \in G_p$.

Let now π be an admissible representation of G_p on a vector space V. Then for $\phi \in C_c^\infty(G_p)$ the operator $\pi(\phi) \in \mathrm{End}_{\mathbf{C}}(V)$ is defined by the integral

$$\pi(\phi)v = \int_{G_p} \phi(g)\pi(g)(v)dg. \tag{2.14}$$

From the smoothness of π it follows that for each $v \in V$ the stabilizer of v is an open subgroup of G_p, therefore for any $\phi \in C_c^\infty(G_p)$ the function

$$G_p \ni g \to \phi(g)\pi(g)(v) \in G_p$$

is locally constant and compactly supported and the integral 2.14 is a finite sum. Moreover, if ϕ is bi–invariant by the open compact subgroup K, we have that $\pi(\phi)(v)$ belongs to the space V^K of K–invariant vectors of V, in particular, by the admissibility of π, we see that $\pi(\phi)$ has finite rank.

The map $C_c^\infty(G_p) \ni \phi \to \pi(f) \in \mathrm{End}(V)$ defines a representation of $C_c^\infty(G_p)$ on $\mathrm{End}(V)$, as a direct calculation shows. The Hecke operator $\tilde{T}_p$ is the element of $C_c^\infty(G_p)$ given by the characteristic function of the double coset

$$K_p \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} K_p. \tag{2.15}$$

The Hecke operator acts on the representation space V of π via the endomorphism $\pi(\tilde{T}_p)$, which will also be called Hecke operator. Since $\tilde{T}_p$ is bi–invariant by K_p, one sees that $\pi(\tilde{T}_p)$ preserves the space of K_p–fixed vectors of π.

The double coset 2.15 is the disjoint union of left cosets

$$K_p \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} K_p = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} K_p \bigcup_{0 \le i \le p-1} \begin{pmatrix} p & i \\ 0 & 1 \end{pmatrix} K_p.$$

It follows that if $v \in V^{K_p}$, then

$$\pi(\tilde{T}_p)(v) = \pi\left(\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\right) \cdot v + \sum_{1 \le i \le p-1} \pi\left(\begin{pmatrix} p & i \\ 0 & 1 \end{pmatrix}\right) \cdot v. \tag{2.16}$$

Let now π be an irreducible, admissible, representation of G_p that is unramified. According to proposition 2.2.13 we have that $\pi \simeq \pi(\chi_1, \chi_2)$, for some unramified characters χ_1 and χ_2 of $\mathbf{Q}_p^*$, uniquely determined up to permutation. Moreover, the space π^{K_p} of K_p–fixed vectors of π is one–dimensional and the Hecke operator $\pi(\tilde{T}_p)$ acts on π^{K_p} as multiplication by a certain scalar λ_p, depending on χ_1 and χ_2.

Lemma 2.2.15. *We have that* $\lambda_p = p^{1/2}(\chi_1(p) + \chi_2(p))$.

Proof. Let V be the representation space consisting of the K_p–finite vectors of $\pi = \pi(\chi_1, \chi_2)$ and let $v_0 \in V$ be a nonzero K_p–fixed vector (for example $v_0 = f_0$, defined in section 2.2.4). It is easy to see that $v_0(1_2)$ is nonzero, where 1_2 is the identity element, for v_0 By formula 2.16 we hve that the K_p–fixed vector $\pi(\tilde{T}_p)(f_0)$ is given by

$$\pi(\tilde{T}_p)(f_0)(g) = f_0\left(g\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\right) + \sum_{1 \le i \le p-1} f_0\left(g\begin{pmatrix} p & i \\ 0 & 1 \end{pmatrix}\right).$$

□

2.3 Cuspidal representation of $\mathbf{GL}_2(\mathbf{A})$

2.3.1 Tensor product factorization

We have mentioned at the end of section 2.1.3 that any unitary, irreducible representation π of the global group $G_{\mathbf{A}}$ factors as restricted tensor product of a unique family

π_p of unitary representations of the local groups G_p. Let us explain how the restricted tensor product $\otimes\pi_p$ can be constructed (cf. [16],[15] for more details).

For any prime p, finite or infinite, assume that it is given a unitary representation π_p of G_p on a Hilbert space V_p so that π_p is *unramified* for all primes p that do not belong to a finite set S containing infinity. For each $p \notin S$, pick a unit vector $x_p \in V_p$ that belongs to the line of V_p given by K_p-fixed vectors. Consider the space V_0 defined to be the subspace of the infinite tensor $\otimes_p V_p$ spanned by the vectors $\otimes v_p$ where $v_p = x_p$ for almost all primes p. Then the adelic group $G_{\mathbf{A}}$ acts on each tensor $\otimes v_p$ and on V_0 by linearity. Moreover, the action is unitary with respect to the norm

$$|\otimes v_p| = \Pi_p |v_p|_p,$$

where $|\ |_p$ denotes the norm of V_p. Let $\otimes' V_p$ be the completion of V_0. The resulting representation of $G_{\mathbf{A}}$ on this Hilbert space is denoted by $\otimes\pi_p$.

There is the following basic factorization theorem (cf. [15]):

Theorem 2.3.1. *Let π be an irreducible, unitary representation of $G_{\mathbf{A}}$. Then there exists unitary irreducible representations π_p of G_p for all p, such that π_p is unramified for almost all finite primes p, and π is unitarily equivalent to $\otimes\pi_p$. Furthermore, the local components π_p are uniquely determined by π, up to equivalence.*

We have the following "strong multiplicity one" result due to Jacquet-Langlands

Theorem 2.3.2. *Let (π, V) and (π', V') be two cuspidal representations of $G_{\mathbf{A}}$ in $L_0^2(\psi)$. Suppose for almost all primes p their local components π_p and π'_p are equivalent. Then $(\pi, V) = (\pi', V')$.*

The proof of this theorem is in [22]. It will be used in the next section to show that a cuspidal eigenform corresponds naturally to a unique cuspidal representation of $G_{\mathbf{A}}$.

2.3.2 Modular forms and cuspidal representations

Let $N, k \geq 1$ be integers, $\epsilon : (\mathbf{Z}/N)^* \to \mathbf{C}^*$ a Dirichlet character and $f \in \mathbf{M}_k^0(\Gamma_0(N), \epsilon)$ a cuspidal modular form of type (k, ϵ). Recall that in section 2.1.1 we have associated to ϵ a character ψ_ϵ of $Z_{\mathbf{A}}K(N)$, viewed as a subgroup of $G_{\mathbf{A}}$, and that in section 2.1.3 we have attached to any such f a function $\Phi_f \in L_0^2(\psi_\epsilon)$ satisfying

i) $\Phi(\gamma a) = \Phi(a)$ for all $\gamma \in G_{\mathbf{Q}}$;

ii) $\Phi(a \cdot u(\theta)) = \Phi(a)e^{i\theta\nu}$ for all $u(\theta) \in K_\infty^0$;

iii) $\Phi(a \cdot z \cdot u) = \Phi(a)\psi_\epsilon(zu)$ for all $z \in Z_{\mathbf{A}}$, $u \in K(N)$;

where Φ_f is defined on the connected component of the archimedean component G_∞^0 by $\phi_f \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} = f(x+iy)y^{k/2}$.

We will need the following lemma relating the classical Hecke operator T_p to $\tilde{T}_p$. Denote by $\rho = \rho_{o,\psi_\epsilon}$ the right translation action of $G_{\mathbf{A}}$ on $L_0^2(\psi_\epsilon)$. Observe that the component at p of ϕ_f is a K_p fixed vector

Lemma 2.3.3. *If $p \nmid N$ then $p^{k/2-1}\rho(\tilde{T}_p)\phi_f = \phi_{T_p f}$*

Let now f be a normalized eigenform of $f \in \mathbf{M}_k^0(\Gamma_0(N), \epsilon)$ belonging to the system of eigenvalues (λ_p). Denote by $V(f)$ the closed $G_{\mathbf{A}}$–submodule of $L_0^2(\psi_\epsilon)$ generated by ϕ_f.

Proposition 2.3.4. *The space $V(f)$ is irreducible and therefore defines a cuspidal representation $\pi = \pi_f$ of $G_{\mathbf{A}}$. Moreover, if p is a prime, denote by $\pi_{K,p}$ the admissible representation of G_p arising from the unitary local factor π_p of π. Then*

i) $\pi_{K,\infty}$ is the discrete series D_{k-1} of lowest weight k;

ii) $\pi_{K,p}$ is unramified for any $p \nmid N$, and $\pi_{K,p} \simeq \pi(\chi_1, \chi_2)$, where the unordered pair χ_1, χ_2 of unramified characters of $\mathbf{Q}_p^*$ is determined by

$$\lambda_p = p^{\frac{k-1}{2}}(\chi_1(p) + \chi_2(p)),$$

$$\epsilon(p) = \chi_1(p)\chi_2(p).$$

In the other direction, if (π, V) is an irreducible component of $L_0^2(\psi_\epsilon)$, for some character ϵ of $(\mathbf{Z}/N)^*$, and so that the admissible representation of G_∞ arising from π_∞ is the discrete series D_{k-1}, then we can construct an Hecke cuspidal eigenform f_π in the following way. Let π_p be local component at p of π and V_p the representation space for π_p Let S be the set of finite primes p so that π_p is ramified, and for $p \notin S$ choose a vector $e_p \in V_p$ fixed by K_p and so that relative to this choice we have $\pi = \otimes\pi_p$. For $p \in S$, chose a new vector $e_p \in V_p$ (cf. 2.2.14) for π_p. Let now ϕ be the image in $L_0^2(\psi_\epsilon)$ of the tensor $\otimes e_p$. Then ϕ is a cuspidal function $\phi : G_{\mathbf{Q}} \backslash G_{\mathbf{A}} \to \mathbf{C}$.

CHAPTER 3

MODULAR FORMS MOD P AND GALOIS REPRESENTATIONS

3.1 Introduction

3.1.1 Modular Galois representations

We introduce a fundamental and classical theorem due to Eichler–Shimura, Deligne and Deligne–Serre that links modular forms to Galois representations. Before doing so, we establish the basic notation that will be used throughout the chapter.

If $\bar{\mathbf{Q}}$ is an algebraic closure of the field of rational numbers, then $G_{\mathbf{Q}}$ denotes $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, the absolute Galois group of $\mathbf{Q}$, equipped with its natural Krull topology. We will consider linear Galois representations

$$\rho : G_{\mathbf{Q}} \to \mathrm{GL}_k(V),$$

where V is a *finite* dimensional vector space over a field k. The fields k that will intervene are the complex numbers $\mathbf{C}$, finite extensions $K/\mathbf{Q}_p$ of the field of p-adic numbers and subfields $\mathbf{F}$ of an algebraic closure $\overline{\mathbf{F}}_p$ of the prime field of characteristic p. In each of these cases, k carries a natural topology (discrete if $\mathrm{char}(k) > 0$) and the representation ρ will *always* be assumed *continuous* with respect to the natural topology of $\mathrm{GL}_k(V)$. If k is $\mathbf{C}$ or a subfield of $\overline{\mathbf{F}}_p$ then ρ will have *open* kernel and therefore *finite* image, by compactness of $G_{\mathbf{Q}}$. For $k = \mathbf{C}$, the kernel of ρ is open because $\mathrm{GL}_k(V)$ has a neighborhood of the identity containing no subgroups other than the trivial one. For k a subfield of $\overline{\mathbf{F}}_p$, the same statement holds simply because $\mathrm{GL}_k(V)$ is discrete.

If K is a finite extension of $\mathbf{Q}$ inside $\bar{\mathbf{Q}}$, then $\mathcal{O}_K$ is the ring of integers of K, integral closure of $\mathbf{Z}$ in K. The union of all the $\mathcal{O}_K$'s in $\bar{\mathbf{Q}}$ is the ring $\bar{\mathbf{Z}}$ of algebraic integers. If p is a prime number, then a prime ideal $\mathfrak{p} \subset \bar{\mathbf{Z}}$ of residual characteristic p is the choice, for any finite extension K of $\mathbf{Q}$, of a prime ideal of $\mathcal{O}_K$ above p, made in a compatible way. The field $\bar{\mathbf{Z}}/\mathfrak{p}$ is isomorphic to an algebraic closure $\overline{\mathbf{F}}_p$ of $\mathbf{F}_p$. The decomposition group $D_{\mathfrak{p}}$ is the closed subgroup of $G_{\mathbf{Q}}$ that stabilizes $\mathfrak{p}$. The datum of a prime ideal $\mathfrak{p}$ of $\bar{\mathbf{Z}}$ is equivalent to that of an embedding $\bar{\mathbf{Q}} \to \bar{\mathbf{Q}}_p$, and $D_{\mathfrak{p}}$ in this way can be identified with

$\mathrm{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p)$. The closed subgroup of $D_\mathfrak{p}$ consisting of elements that induce the trivial field automorphism at the residual level is the inertia group at $\mathfrak{p}$, denoted by $I_\mathfrak{p}$. The exact sequence

$$1 \to I_\mathfrak{p} \to D_\mathfrak{p} \to \mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p) \to 1,$$

defines the canonical element of $D_\mathfrak{p}/I_\mathfrak{p}$, denoted by $\mathrm{Frob}_\mathfrak{p}$, corresponding to the Frobenius automorphism $x \to x^p$ on $\overline{\mathbf{F}}_p$.

The representation ρ is unramified at p if $\rho(I_\mathfrak{p})$ is the trivial subgroup of $\mathrm{GL}_k(V)$, for some, and therefore any, choice of a prime $\mathfrak{p}$ of $\bar{\mathbf{Z}}$ above p. In this case $\rho(\mathrm{Frob}_\mathfrak{p})$ is well defined and its conjugacy class depends only on the rational prime p, and not on the choice of the prime $\mathfrak{p}$ of $\bar{\mathbf{Z}}$.

Theorem 3.1.1. *Let f be a nonzero classical modular form of type (k, ϵ) for $\Gamma_0(N)$. Assume that f is an eigenvector for the Hecke operators T_ℓ, for all $\ell \nmid N$, with eigenvalues a_ℓ. Let K be a finite extension of $\mathbf{Q}$ containing a_ℓ and $\epsilon(\ell)$, for all $\ell \nmid N$. Let $\mathfrak{p}$ be a finite place of K of residual characteristic p, and let $K_\mathfrak{p}$ be the completion of K at $\mathfrak{p}$. Then there exists a unique, semisimple, representation*

$$\rho_{f,\mathfrak{p}} : G_\mathbf{Q} \to GL_2(K_\mathfrak{p})$$

which is unramified outside pN and so that

$$tr(\rho_{f,\mathfrak{p}}(Frob_\ell)) = a_\ell \qquad and \qquad \det(\rho_{f,\mathfrak{p}}(Frob_\ell)) = \epsilon(\ell)\ell^{k-1}, \tag{3.1}$$

for all primes $\ell \nmid pN$.

The theorem was first proved by Eichler–Shimura in the case $k = 2$ (cf. [13],[53]), then Deligne generalized it to any weight $k \geq 2$ (cf. [9]) and the remaining case $k = 1$ was proved by Deligne–Serre (cf. [11]). The image of $\rho_\mathfrak{p}$ is a closed subgroup of $\mathrm{GL}_2(K_\mathfrak{p})$ which is infinite if and only if $k > 1$. It follows from the second condition of 3.1 that

$$\det \rho_{f,\mathfrak{p}} = \epsilon\chi_p^{k-1},$$

where χ_p is the p–adic cyclotomic character of $G_\mathbf{Q}$, describing its action on the roots of unity μ_{p^n}, and epsilon is regarded as a character of $G_\mathbf{Q}$ via the canonical isomorphism

$$G_\mathbf{Q}^{ab} \xrightarrow{\sim} \hat{\mathbf{Z}}^*, \tag{3.2}$$

where $G_\mathbf{Q}^{ab}$ is the quotient of $G_\mathbf{Q}$ by the *closure* of its commutator subgroup. The representation $\rho_{f,\mathfrak{p}}$ is *odd*, meaning that, if c is a complex conjugation of $G_\mathbf{Q}$ then $\det \rho_{f,\mathfrak{p}}(c) = -1$. This is because c is identified with -1 by 3.2, and necessarily $\epsilon(-1) = (-1)^k$.

Observe that the theorem does not just state the existence of a single Galois representation $\rho_{f,\mathfrak{p}}$, but rather of a *compatible system* of two–dimensional Galois representations, in the terminology of [43], with exceptional set S given by the primes p dividing the level N of the form f. The point is that the conditions 3.1 imposed on $\rho_{f,\mathfrak{p}}(\mathrm{Frob}_\ell)$, that uniquely characterize $\rho_{f,\mathfrak{p}}$, are *independent* of the prime $\mathfrak{p}$ of K considered.

If f is an Eisenstein series, then the representation $\rho_{f,\mathfrak{p}}$ is the direct sum of two one–dimensional characters of $G_{\mathbf{Q}}$. Its existence follows from the explicit description of the systems of Hecke eigenvalues that may occur in this situation. The theorem in this easier case was known to Hecke.

The formulation of the theorem for $k > 2$ is based on a conjecture that Serre made in 1968 (cf. [42]), the case $k = 2$ being already known at the time. More precisely, Serre predicted the existence of $\rho_{f,\mathfrak{p}}$ in the special case where the modular form f considered is the unique cuspidal eigenform of weight 12 for $\mathrm{SL}_2(\mathbf{Z})$, the Ramanujan Δ function.

3.1.2 Serre's modularity conjecture

Let f be a cusp form of type (k, ϵ) on $\Gamma_0(N)$ so that $f|T_\ell = a_\ell f$, for all $l \nmid N$, and let

$$\rho_{f,\mathfrak{p}} : G_{\mathbf{Q}} \to \mathrm{GL}_2(K_{\mathfrak{p}})$$

be the p–adic compatible system of Galois representations attached to f by theorem 3.1.1, in the notation of the previous section. If $\mathcal{O}_{\mathfrak{p}}$ is the ring of integers of $K_{\mathfrak{p}}$, then there exists a $\mathcal{O}_{\mathfrak{p}}$–lattice of $K_{\mathfrak{p}}^2$ that is $G_{\mathbf{Q}}$–stable (cf. [43]). Therefore, after a suitable change of basis, the representation $\rho_{f,\mathfrak{p}}$ is valued in $\mathrm{GL}_2(\mathcal{O}_{\mathfrak{p}})$. Let now $\mathfrak{m}_{\mathfrak{p}}$ be the maximal ideal of the local ring $\mathcal{O}_{\mathfrak{p}}$ and $k_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}}$ the residue field of K at $\mathfrak{p}$.

Theorem 3.1.2. *For any f and $\mathfrak{p}$ as above, there exists a unique semisimple, odd, mod p, Galois representation*

$$\bar{\rho}_{f,\mathfrak{p}} : G_{\mathbf{Q}} \to GL_2(k_{\mathfrak{p}})$$

which is unramified outside pN and so that

$$tr(\bar{\rho}_{f,\mathfrak{p}}(Frob_\ell)) \equiv a_\ell \mod \mathfrak{p} \quad and \quad \det(\bar{\rho}_{f,\mathfrak{p}}(Frob_\ell)) \equiv \epsilon(\ell)\ell^{k-1} \mod \mathfrak{p}, \tag{3.3}$$

for all primes $\ell \nmid pN$.

The representation $\bar{\rho}_{f,\mathfrak{p}}$ is the semisimplification of the reduction mod $\mathfrak{m}_{\mathfrak{p}}$ of

$$\rho_{f,\mathfrak{p}} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathcal{O}_{\mathfrak{p}}),$$

and it is independent of the integral model chosen. Oddness here means the same thing as in the previous section, for $c \in G_{\mathbf{Q}}$ complex conjugation we have $\det \rho_{f,\mathfrak{p}}(c) = (-1) \in \mathbf{F}_p^*$. The condition is vacuous for $p = 2$ and in all other cases implies that $\rho_{f,\mathfrak{p}}$ is irreducible if and only if it is absolutely irreducible.

Definition 3.1.3. Let p be any prime number and $\bar{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ a semisimple, odd Galois representation. We will say that $\bar{\rho}$ is *modular* if there exists f as above so that $\bar{\rho}$ is isomorphic to $\rho_{f,\mathfrak{p}} \otimes \overline{\mathbf{F}}_p$, for a prime $\mathfrak{p}$ of residual characteristic p.

Serre in the earlier 70s started to develop his influential modularity conjecture

Conjecture 3.1.4. *Let p be a prime number and $\bar{\rho} : G_{\mathbf{Q}} \to GL_2(\overline{\mathbf{F}}_p)$ be a semisimple, odd Galois representation of $\mathbf{Q}$. Then $\bar{\rho}$ is modular.*

In its first written appearance in 1975, the conjecture (cf. [44]) was stated in the special case where $\bar{\rho}$ is unramified outside p. The conjecture in its full formulation came later, in 1986 (cf. [45]), where Serre went further and indicated a recipe to identify the type (k, ϵ) of a modular form f which should give rise to $\bar{\rho}$ by the procedure that we had described. The level N is the prime to p part of the Artin conductor of $\bar{\rho}$, defined as in characteristic zero, the definition of the weight is more delicate, and it is meant to be as small as possible (cf. Serre, loc. cit). In the case $p = 2$, Serre's definition of the weight actually needs to be modified (cf. [14]).

Theorem 3.1.5. *Serre's modularity conjecture is true.*

Khare in February 2005 proved the level one case of Serre's conjecture (cf. [28]), i.e., the case where $\bar{\rho}$ is unramified outside p, using a technique that he had started to develop with Winterberger [31]. The general case was then proved by Khare–Winterberger soon after. The proof of the modularity conjecture uses the work of a large number of mathematicians such as Ribet, Taylor, Wiles, Mazur, Deligne, Kisin, Carayol and others.

An immediate corollary of Serre's conjecture, which is central to our thesis, is the following finiteness theorem:

Theorem 3.1.6. *Let p be prime and $N > 0$ prime to p. Then, up to isomorphism, there exist only finitely many two–dimensional, irreducible, odd Galois representations $\bar{\rho} : G_{\mathbf{Q}} \to GL_2(\overline{\mathbf{F}}_p)$ of Serre's conductor N.*

One may therefore ask for a refinement of this question, as stressed in [29]. More precisely given an integer $N > 0$, how many absolutely irreducible, two–dimensional, odd, mod p representations of $G_{\mathbf{Q}}$ of Serre's conductor N are there? This is the guiding problem of our thesis. Let us denote this finite number by $R_N(p)$. Even though we are far from getting any definite answer to question above, we will propose a conjectural formula predicting what the asymptotics with p of $R_N(p)$ should be. We also collect computational evidence for the formula in the level 1 case.

The main ingredient that is used in the argument supporting the numerics for $R_N(p)$ will be, again, a theorem of Serre, which relates mod p systems of Hecke eigenvalues coming from modular forms to those coming from certain automorphic forms on the multiplicative group of the quaternion algebra over $\mathbf{Q}$ ramified exactly at p and infinity.

3.2 Modular forms mod p

3.2.1 Congruences between Eisenstein Series

For any prime number p, we denote by ν_p the associated additive valuation of $\mathbf{Q}$ normalized by the equality $\nu_p(p) = 1$. If $f = \Sigma_{n\geq 0} a_n q^n \in \mathbf{Q}[[q]]$ is a power series with coefficients in $\mathbf{Q}$ we will say that f is p–integral if $\nu_p(a_n) \geq 0$ for all n. In this case f defines a power series $\tilde{f} \in \mathbf{F}_p[[q]]$ obtained by reducing its coefficients mod p. If $g \in \mathbf{Q}[[q]]$ is also p–integral, then we will say that $f \equiv g \bmod p$ if $\tilde{f} - \tilde{g} = 0$ in $\mathbf{F}_p[[q]]$.

We are going to see how classical congruences between Bernoulli numbers can be interpreted as congruences between Eisentein series. Let us first recall the Fourier expansion at infinity of the Eisenstein series for $\mathrm{SL}_2(\mathbf{Z})$ given in formulas 1.5 and 1.6

$$G_k = -\frac{b_k}{2k} + \sum_{n\geq 1} \sigma_{k-1}(n) q^n,$$

$$E_k = -\frac{2k}{b_k} G_k = 1 - \frac{2k}{b_k} \sum_{n\geq 1} \sigma_{k-1}(n) q^n,$$

where b_k is the k–th Bernoulli number, defined in 1.4, and $\sigma_h(n) = \sum_{0<d|n} d^h$.

Theorem 3.2.1. *Let m and n be even integers > 0. Then*
i) if $p - 1 \nmid n$, then $\nu_p(b_n/n) \geq 0$;
ii) if $n \equiv m \not\equiv 0 \bmod (p-1)$, then $b_n/n \equiv b_m/m \bmod p$.

Proof. The proof can be found in [33], X, th. 1.1. □

The theorem implies

Proposition 3.2.2. *Let $p > 2$ be a prime number and $k > 2$ an even integer so that $p - 1 \nmid k$. Let k_0 be the unique integer j so that $1 < j < p - 1$ and $j \equiv k \ mod\ (p - 1)$. Then, $\nu_p(G_k) = 0$ and $G_k \equiv G_{k_0} \ mod\ p$.*

Proof. From theorem 3.2.1 and the formula for the q–expansion of G_k, we immediately see that all the Fourier coefficients of G_k are p–integral, that is $\nu_p(G_k) \geq 0$. To show that $\nu_p(G_k) = 0$ we can simply remark that the coefficient of q in the expansion of G_k is 1. The second part of the proposition follows from theorem 3.2.1 and from the congruence

$$\sigma_{k-1}(n) = \sigma_{k_0-1}(n) \mod p,$$

valid for all integers n, since $k, k_0 \neq 1$. □

In the case where $p - 1|k$ the Clausen-von Staut theorem says

Theorem 3.2.3. *Let n be an even integer divisible by $p-1$ ($p = 2$ is allowed here). Then $\nu_p(b_n) = -1$.*

Proof. For the proof cf. [33], X, th. 2.1. □

Therefore it is easy to conclude that

Proposition 3.2.4. *Let p be a prime number and $k > 2$ an even integer so that $p - 1|k$. Then, $\nu_p(G_k) = -1 - \nu_p(2k)$ and $\nu_p(E_k - 1) = 1 + \nu_p(2k)$. In particular, for $p > 3$, we have $E_{p-1} \equiv 1 \ mod\ p$.*

We will see in the next section that this congruence is essentially the only one to consider when studying mod p modular forms.

Remark 3.2.5. Let k be an even integer so that $p - 1|k$. Then, the last proposition says that

$$E_k \equiv 1 \mod p^m \Leftrightarrow k \equiv 0 \mod (p-1)p^{m-1}, \quad \text{if } p \geq 2$$

$$E_k \equiv 1 \mod 2^m \Leftrightarrow k \equiv 0 \mod 2^{m-2}.$$

This is a special case of the following general fact, shown by Serre (cf. [46], Théorème 1).

Theorem 3.2.6. *Let f and g be modular forms in for $SL_2(\mathbf{Z})$ of respective weights k and k' with rational, p–integral coefficients. If $f \equiv g \ mod\ p^m$ then*

$k \equiv k' \ mod\ (p-1)p^{m-1}$ *if* $p \geq 3$ *and*

$k \equiv k' \ mod\ 2^{m-2}$ *if* $p = 2$.

This theorem plays an important role in the definition of the weight of a *p–adic modular form* (cf. Serre, loc. cit.)

3.2.2 The algebra of mod p modular forms

Let p be a prime number, and $N > 0$ an integer prime to p. For any $k \geq 0$, consider the space $\mathbf{M}_k(\Gamma_1(N), \mathbf{F}_p)$ of modular forms of weight k over the field $\mathbf{F}_p$. The space

$$\oplus_{k\geq 0}\mathbf{M}_k(\Gamma_1(N), \mathbf{F}_p)$$

is a graded algebra, where $\mathbf{M}_0(\Gamma_1(N), \mathbf{F}_p) = \mathbf{F}_p$. Its Krull dimension is two (cf. [17]). For any fixed weight k, the q–expansion map

$$\mathbf{M}_k(\Gamma_1(N), \mathbf{F}_p) \to \mathbf{F}_p[[q]]$$

is injective. Consider the ring homomorphism

$$\oplus_{k\geq 0}\mathbf{M}_k(\Gamma_1(N), \mathbf{F}_p) \to \mathbf{F}_p[[q]]$$

obtained by patching together the q–expansion morphisms for a fixed k. This map is not injective in general since, for example for $p > 3$,

$$\tilde{E}_{p-1} = 1,$$

as already remarked in the previous section (corollary 3.2.4).

Definition 3.2.7. The algebra $\mathbf{M}(\Gamma_1(N), \mathbf{F}_p)$ of modular forms is the subalgebra of $\mathbf{F}_p[[q]]$ defined by the image of the q–expansion map at infinity

$$\oplus_{k\geq 0}\mathbf{M}_k(\Gamma_1(N), \mathbf{F}_p) \to \mathbf{F}_p[[q]].$$

Proposition 3.2.8. *Let $p > 3$, the modular form $\tilde{E}_{p-1} =\in \mathbf{M}_{p-1}(\Gamma_1(N), \mathbf{F}_p)$ coincides with the Hasse invariant. More precisely, for any scheme S over $\mathbf{F}_p$ and any pair (E, α), where E is an elliptic curve over S and $\alpha : \mu_N \to E[N]$ an embedding of $\mathbf{F}_p$–group schemes, we have that $\tilde{E}_{p-1}(E, \alpha)$ is the Hasse invariant of E in $H^0(E, \underline{\omega}_E^{p-1})$.*

Proof. The Hasse invariant of the pair (E, α) depends actually only on E and is defined as follows (cf. [26], I, or [27] 12.4): after Zariski localizing, we may assume that $S = \mathrm{Spec}(R)$ is affine, where R is a $\mathbf{F}_p$–algebra, and that the R–module $H^0(E, \underline{\omega}_E)$ of invariant differentials on E is free, necessarily of rank one. Let then $\omega \in H^0(E, \underline{\omega}_E)$ be any basis element and let $\eta \in H^1(E, \mathcal{O}_E)$ be the Serre dual basis element, where $\mathcal{O}_E$ is the structure sheaf on E. Then the (absolute) Frobenius endomorphism of $\mathcal{O}_E$ induces and a p–linear map

$$F : H^1(E, \mathcal{O}_E) \to H^1(E, \mathcal{O}_E),$$

and we must have $F(\eta) = A(E, \omega)\eta$ in $H^1(E, \mathcal{O}_E)$, for some $A(E, \omega)$. For any $\lambda \in R^*$ we see that $A(E, \lambda\omega) = \lambda^{1-p}A(E, \omega)$, and the invariant form $A(E, \omega)\omega^{p-1}$ in $H^0(E, \underline{\omega}_E^{p-1})$ depends only on E/R, this is the Hasse invariant A as modular form of weight $p-1$ in $\mathbf{M}_{p-1}(\Gamma_1(N), \mathbf{F}_p)$. A calculation on the Tate curve shows that the q–expansion at infinity (in fact at *any* cusp) of A is constant and equal to 1 (cf. [27] th. 12.4.2, §8.8). Now, A and $\tilde{E}_{p-1}$ are elements of $\mathbf{M}_{p-1}(\Gamma_1(N), \mathbf{F}_p)$ with the same q–expansion, therefore they must coincide. □

Let $X(N) = X_1^0(N)/\overline{\mathbf{F}}_p$ be the affine, mod p, modular curve and $\mathcal{E}$ the universal elliptic curve, for $N > 4$. The Hasse invariant A is an element of $H^0(X(N), \underline{\omega}_{\mathcal{E}}^{p-1})$.

Proposition 3.2.9. *The Hasse invariant has only simple zeros occurring precisely at the supersingular fibers.*

Proof. It is well known that the Hasse invariant is zero exactly on the supersingular elliptic curves (cf. [27] 12.3.6). A possible proof of the second part of the proposition that uses the differential equation satisfied by A is in [21]. □

Theorem 3.2.10. *The kernel of the q–expansion map*

$$\oplus_{k \geq 0}\mathbf{M}_k(\Gamma_1(N), \mathbf{F}_p) \to \mathbf{F}_p[[q]]$$

is the principal ideal generated by $A - 1$, where $A \in \mathbf{M}_{p-1}(\Gamma_1(N), \mathbf{F}_p)$ is the Hasse invariant.

Proof. Denote the kernel of the q–expansion map by $\mathfrak{p}$, it is a prime ideal since $\mathbf{F}_p[[q]]$ is a domain. It is clear that $\mathfrak{p}$ contains the principal ideal $(A - 1)$, we need to show that equality holds. The element $A - 1$ is *absolutely irreducible*, since A does not have

multiple factors (cf. [21] or [47]), and the principal ideal $(A-1)$ is prime. The ideal $\mathfrak{p}$ is not maximal since the algebra $\mathbf{M}(\Gamma_1(N),\mathbf{F}_p)$ is not finite, in fact, for any even $k>2$ we have that the monomials $\tilde{G}_4^a\tilde{G}_g^b$, with $4a+6b=k$, are $\mathbf{F}_p$–independent. If now the prime ideal generated by $(A-1)$ were properly contained in $\mathfrak{p}$ then we would have that the dimension of $\oplus_{k\geq 0}\mathbf{M}_k(\Gamma_1(N),\mathbf{F}_p)$ is greater than two, which is a contradiction. $\square$

The theorem says that the algebra of mod p modular forms can be described as

$$\mathbf{M}(\Gamma_1(N),\mathbf{F}_p)\simeq\oplus_{k\geq 0}\mathbf{M}_k(\Gamma_1(N),\mathbf{F}_p)/(A-1),$$

where A is a certain modular form of weight $p-1$ (it is $\tilde{E}_{p-1}$ when $p>3$). The ring $\mathbf{M}(\Gamma_1(N),\mathbf{F}_p)$ is graded by $\mathbf{Z}/(p-1)$, for $h\in\mathbf{Z}/(p-1)$ we have that

$$\mathbf{M}(\Gamma_1(N),\mathbf{F}_p)=\oplus_{h\in\mathbf{Z}/(p-1)}\mathbf{M}^{(h)}(\Gamma_1(N),\mathbf{F}_p),$$

where $\mathbf{M}^{(h)}(\Gamma_1(N),\mathbf{F}_p)$ is the direct limit

$$\mathbf{M}^{(h)}(\Gamma_1(N),\mathbf{F}_p)=\lim_{n\to\infty}\mathbf{M}_{k+n(p-1)}(\Gamma_1(N),\mathbf{F}_p),$$

where $k\equiv h \bmod (p-1)$, $0\leq k\leq p-2$ and where the maps

$$\mathbf{M}_{k+n(p-1)}(\Gamma_1(N),\mathbf{F}_p)\to\mathbf{M}_{k+(n+1)(p-1)}(\Gamma_1(N),\mathbf{F}_p)$$

are multiplication by A. Alternatively, one may consider the previous limit simply as a reunion, where the inclusions

$$\mathbf{M}_{k+n(p-1)}(\Gamma_1(N),\mathbf{F}_p)\subset\mathbf{M}_{k+(n+1)(p-1)}(\Gamma_1(N),\mathbf{F}_p),$$

are obtained by identifying modular forms of given weights with their q-expansion. From now on, the space $\mathbf{M}_k(\Gamma_1(N),\mathbf{F}_p)$ will be considered as subspace of $\mathbf{M}^{(k)}(\Gamma_1(N),\mathbf{F}_p)$.

Let k be a integer with $0\leq k\leq p-2$, all the Hecke operators T_l and U_q, for $l\nmid pN$ and $q|N$, act on the filtered space

$$\mathbf{M}_k\subset\mathbf{M}_{k+(p-1)}\subset\ldots\subset\mathbf{M}^{(k)}$$

respecting the filtration. More precisely, the action of each of the operators listed above on $\mathbf{M}_{k+(n+1)(p-1)}$ extends the action of the operator on the subspace $\mathbf{M}_{k+n(p-1)}$, for all $n\geq 0$. This is clear, the formulas defining the actions of the Hecke operators above on q-expansion, depend only on the class of k mod $(p-1)$. Another way to say this is

that T_l and U_q, for $l \nmid pN$ and $q|N$, commute with A. However, this is not true for the operator T_p, as it definition on q-expansion of forms on $\mathbf{M}_k$ depends on whether $k = 1$ or not. Whenever we will speak of T_p acting on the algebra of modular forms, we will assume that its defining equation is that for modular forms of weight bigger than one, if $f = \sum_{n\geq 0} a_n q^n$, then

$$f|T_p = \sum_{n\geq 0} a_{pn} q^n.$$

Since this formula is analogous to that defining the operators U_q, it is customary to denote T_p by U_p. In conclusion, all the Hecke operators act on the ring $\mathbf{M}(\Gamma_1(N), \mathbf{F}_p)$.

3.2.3 The operators V and θ

Besides Hecke operators, there are two endomorphisms of $\mathbf{M}(\Gamma_1(N), \mathbf{F}_p)$ that exist only in characteristic p. The endomorphism V is the Frobenius map, existing on any $\mathbf{F}_p$ algebra, given by $f|V = f^p$. If $f = \sum_{n\geq 0} a_n q^n$ then the effect of V on Fourier expansion is

$$f|V = \sum_{n\geq 0} a_n q^{pn}.$$

The unique $\overline{\mathbf{F}}_p$ linear extension of V on $\mathbf{M}(\Gamma_1(N), \overline{\mathbf{F}}_p)$ has the same defining formula on q-expansion and satisfies $(f|V)^\sigma = (f)^p$, where $g^\sigma = \sum_{n\geq 0} b_n^p q^n$ is the conjugate of $g = \sum_{n\geq 0} b_n q^n$ with respect to the absolute Frobenius automorphism $\sigma \in \mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$. The operator V sends the space $\mathbf{M}_k(\Gamma_1(N), \mathbf{F}_p)$ to $\mathbf{M}_{pk}(\Gamma_1(N), \mathbf{F}_p)$ (this map is actually the reduction mod p of the map which sends a form $f \in \mathbf{M}_k(\Gamma_1(N), \mathbf{Z}[1/N])$ to $f^p \in \mathbf{M}_{pk}(\Gamma_1(N), \mathbf{Z}[1/N])$), in particular V preserves the $\mathbf{Z}/(p-1)$ grading. The operator V commutes with all the Hecke operators T_ℓ, $\ell \nmid pN$ and U_q, $q|N$, as it can be checked on q- expansion.

The operator θ is defined to be the restriction to $\mathbf{M}(\Gamma_1(N), \overline{\mathbf{F}}_p)$ of the derivation

$$q\frac{d}{dq} : \mathbf{F}_p[[q]] \to \mathbf{F}_p[[q]]$$

sending a formal series $\sum_{n\geq 0} a_n q^n$ to $\sum_{n\geq 1} n a_n q^n$.

Proposition 3.2.11. *The derivation $q\dfrac{d}{dq}$ preserves the ring of modular forms. If if $f \in \mathbf{M}_k(\Gamma_1(N), \overline{\mathbf{F}}_p)$ then $f|\theta \in \mathbf{M}_{k+p+1}(\Gamma_1(N), \overline{\mathbf{F}}_p)$.*

The proposition essentially follows from a theorem of Ramanujan (cf. [47] 1.4 for $N = 1$, [26] in general).

If $f \in \mathbf{M}_k(\Gamma_1(N), \overline{\mathbf{F}}_p)$ then we write $\theta(f)$ for the modular form $q\frac{d}{dq}f$. We will need more precise information about the action of V and θ on the filtered spaces $\mathbf{M}^{(h)}(\Gamma_1(N), \mathbf{F}_p)$. To this purpose, we define the *filtration* of a modular form.

Definition 3.2.12. Let $f \in \mathbf{M}^{(h)}(\Gamma_1(N), \mathbf{F}_p)$ be a nonzero mod p modular form. The filtration $w(f)$ of f is the least integer j so that $f \in \mathbf{M}_j(\Gamma_1(N), \mathbf{F}_p)$. Set $w(0) = -\infty$.

Proposition 3.2.13. *Let $f \in \mathbf{M}_k(\Gamma_1(N), \mathbf{F}_p)$ with $w(f) = k$. Then*
i) $w(f|V) = pk$;
ii) $w(\theta(f)) \leq k + p + 1$, equality holds if and only if $p \nmid k$.

For the proof cf. Katz, loc. cit.

The operator θ does not commute with the Hecke operators. We have

$$(\theta f)|T_\ell = \ell\theta(f|T_\ell),$$

$$(\theta f)|U_q = q\theta(f|U_q),$$

$$(\theta f)|U_p = \theta(f|V) = 0,$$

as it can be checked on q-expansion. In particular, if f is a common eigenvector for all the T_ℓ's with eigenvalues (λ_ℓ), then $g = \theta(f)$ is also a common eigenvector of the T_ℓ with eigenvalues (μ_ℓ) where $\mu_\ell = \ell\lambda_\ell$. From the representation theoretical point of view the action of θ correspond to that of the twist by the mod p cyclotomic character χ_p. If ρ_f and ρ_g are the mod p representations associated to f and g, then we have $\rho_g \simeq \rho_f \otimes \chi_p$.

3.2.4 Congruence primes for τ

Swinnerton-Dyer and Serre have shown how the congruences satisfied by the coefficient of the Ramanujan Δ function can be explained in terms of the *images* in $\mathrm{GL}_2(\mathbf{F}_p)$ of the mod p Galois representations attached to it by theorem 3.1.2. Moreover, in a precise sense, they show that τ does not satisfy congruences modulo any other primes. This is perhaps the motivation behind their study of the structure of the algebra of mod p modular forms. In this section we quickly summarize their work, for the proofs we refer to [55].

Let p be a prime number and $\Delta = \sum_{n\geq 1}\tau(n)q^n$ the Ramanujan Δ function. By theorem 3.1.1 there exists a unique, semisimple, odd, Galois representation

$$\rho_p : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{Z}_p)$$

that is unramified outside p and so that, for any prime $\ell \neq p$, satisfies

$$\mathrm{tr}(\rho_p(\mathrm{Frob}_\ell)) = \tau(\ell) \qquad \text{and} \qquad \det \circ \rho_p = \chi_p^{11},$$

were χ_p denotes the p-adic cyclotomic character. Denote by $\bar{\rho}_p$ the mod p representation obtained from ρ_p by reduction of the coefficients.

Definition 3.2.14. A prime number p is a congruence prime for Δ if the image of ρ_p does not contain $\mathrm{SL}_2(\mathbf{Z}_p)$.

The terminology used in the definition is justified by the following

Proposition 3.2.15. *Let p be a prime which is not a congruence prime for Δ, and let N and N^* be nonempty open sets in $\mathbf{Z}_p$ and $\mathbf{Z}_p^*$ respectively. Then the set of primes ℓ for which $\ell \in N^*$ and $\tau(\ell) \in N$ has positive density.*

Therefore, the search of primes p so that Δ satisfies a congruence modulo p can be confined to those for which the image of ρ_p does not contain $\mathrm{SL}_2(\mathbf{Z}_p)$.

Proposition 3.2.16. *Let p be a prime > 3. Then p is a congruence prime if and only if the image of $\bar{\rho}_p$ does not contain $SL_2(\mathbf{F}_p)$.*

The condition is clearly sufficient. The necessity is proven in [55], lemma 1.

This result is not valid for $p = 2, 3$. However, in both cases the image of $\bar{\rho}_p$ does not contain $\mathrm{SL}_2(\mathbf{F}_p)$ and therefore 2 and 3 are congruence primes for Δ.

The following proposition determines the possibilities for the image of $\bar{\rho}_p$ if p is congruence prime.

Proposition 3.2.17. *Let p be a congruence prime for Δ. Let $G = Im(\bar{\rho}_p)$ and H be the projective image of G in $PGL_2(\mathbf{F}_p)$. Then exactly one of the following possibility occur:*
i) G is contained in a Borel subgroup of $GL_2(\mathbf{F}_p)$;
ii) G is contained in the normalizer of a Cartan subgroup and it is not abelian;
iii) H is isomorphic to S_4.

The proof in [55] is done by first classifying all the subgroups of $\mathrm{GL}_2(\mathbf{F}_p)$ that do not contain $\mathrm{SL}_2(\mathbf{F}_p)$. The fact that $\bar{\rho}_p$ has odd determinant and some simple ramification arguments rule out few possibilities for G from the list previously obtained.

Each of the three cases above for the image of $\bar{\rho}_p$ correspond to a specific congruence modulo p that $\tau(\ell)$ satisfies for ℓ prime. A congruence prime p for Δ will be called, accordingly, of type *i*), *ii*) or *iii*).

Proposition 3.2.18. *Let p be a congruence prime for Δ. Then the three cases of proposition 3.2.17 imply respectively the following congruences for $\tau(\ell)$, where ℓ is prime*
i) there exists an integer m so that $\tau(\ell) \equiv \ell^m \sigma_{11-2m}(\ell)$ (mod p) for all $\ell \neq p$;
ii) $\tau(\ell) \equiv 0$ (mod p) whenever $(\frac{\ell}{p}) = -1$, i.e. ℓ is not a square mod p;
iii) $\ell^{-11}\tau(\ell) \equiv 0, 1, 2$ or 4 mod p for all $\ell \neq p$.

Using the multiplicative properties of τ one can see that the congruences in case *i*) and *ii*) are valid for all integers n prime to p. For congruences modulo higher powers of p we refer to Swinnerton-Dyer, loc. cit.

Swinnerton-Dyer and Serre provide explicit bound for congruence primes for Δ and show that

Theorem 3.2.19. *The primes 2, 3, 5, 7 and 691 are the only congruence primes for Δ of type i), 23 is the only congruence prime of type ii) and there are no congruence primes for Δ of type iii).*

We conclude the section saying few more words about the congruence prime $p = 23$. The imaginary quadratic field $K = \mathbf{Q}(\sqrt{-23})$ has class number 3, as it can be easily shown by counting how many reduced quadratic forms of discriminant -23 are there (cf. [48]). Consider the polynomial $f(x) = x^3 - x - 1$, let α be one of its roots. The discriminant of f is -23 and it is easy to see that $\mathbf{Q}(\alpha)$ contains two primes above 23, where one of which is ramified with ramification index 2 and the other is unramified. Moreover, the splitting field L of $f(x)$ contains K since the discriminant of a number field is a square in its Galois closure. All of this implies that L/K is everywhere unramified, therefore L is the Hilbert Class Field of K. Moreover, the Galois group $G = G(L/\mathbf{Q})$ is the permutation group in three letters S_3, the subgroup $G(L/K)$ is cyclic of order 3.

Let $\delta : G(L/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{Z})$ be the standard two–dimensional irreducible representation of S_3 obtained from the permutation representation $\pi : G(L/\mathbf{Q}) \to \mathrm{GL}_3(\mathbf{Z})$ by

taking the quotient by the unique invariant line. We see that for any $\sigma \in G(L/\mathbf{Q})$ we have $\mathrm{tr}(\pi(\sigma)) = \mathrm{tr}(\delta(\sigma)) - 1$. It follows that $\mathrm{tr}(\delta(\sigma)) = 2, 0$ or -1, respectively, according to whether σ is the identity, a 2–cycle or a 3–cycle of S_3.

We are now left to decide, for any prime $\ell \neq 23$, what is the conjugacy class in $G(L/\mathbf{Q})$ of the Frobenius element Frob_ℓ. Using the general properties of the Hilbert Class Field and the Quadratic Reciprocity Law, one can show that
Frob_ℓ is the identity $\Leftrightarrow \ell = u^2 + 23v^2$;
Frob_ℓ has order two $\Leftrightarrow \ell$ is not a quadratic residue mod 23;
Frob_ℓ has order three $\Leftrightarrow \ell$ is a quadratic residue mod 23 and it is not of the form u^2+23v^2.

Reducing the above congruences for $\mathrm{tr}(\mathrm{Frob}_\ell)$ mod 23, we obtain precisely the congruences satisfied by $\tau(\ell)$ mod 23. Therefore we conclude that the reduction of δ mod 23 is isomorphic to $\tilde{\rho}_{23}$.

3.2.5 Finiteness of systems of Hecke eigenvalues mod p

Recall that, by definition, a system Φ of Hecke eigenvalues mod p arising from the space $\mathbf{M}_k(\Gamma_1(N), \overline{\mathbf{F}}_p)$ is a collection (λ_ℓ) of elements of $\overline{\mathbf{F}}_p$ indexed by primes ℓ not dividing N, so that there exists a nonzero modular form $f = \sum_{n\geq 0} a_n q^n \in \mathbf{M}_k(\Gamma_1(N), \overline{\mathbf{F}}_p)$ with $f|T_\ell = \lambda_\ell f$, for all $\ell \nmid N$. Moreover, if h is any integer we denote by $\Phi^{(h)}$ the system deduced from Φ by h repeated twists. So that the ℓ-th eigenvalue of $\Phi^{(h)}$ is $\ell^h \lambda_\ell$.

In contrast to the characteristic zero case we have the following theorem

Theorem 3.2.20. *There are only finitely many systems of Hecke eigenvalues mod p that arise from the algebra of mod p modular forms $\mathbf{M}(\Gamma_1(N), \overline{\mathbf{F}}_p)$.*

Proof. For any $\ell \nmid pN$, the operator T_ℓ preserves the filtration

$$\mathbf{M}_{k-(p-1)}(\Gamma_1(N), \overline{\mathbf{F}}_p) \subset \mathbf{M}_k(\Gamma_1(N), \overline{\mathbf{F}}_p) \subset \ldots \subset \mathbf{M}^{(k)}(\Gamma_1(N), \overline{\mathbf{F}}_p),$$

and acts on each quotient

$$W_k = \mathbf{M}_k(\Gamma_1(N), \overline{\mathbf{F}}_p)/\mathbf{M}_{k-(p-1)}(\Gamma_1(N), \overline{\mathbf{F}}_p).$$

The dimension of W_k is bounded by a constant independent on k, since the dimension of $\mathbf{M}_k(\Gamma_1(N), \overline{\mathbf{F}}_p)$ grows linearly with k (cf. [53] 2.23, 2.25). It follows that there exists a finite extension $\mathbf{F}_q$ of $\mathbf{F}_p$ containing all the systems of eigenvalues arising from the entire algebra $\mathbf{M}(\Gamma_1(N), \overline{\mathbf{F}}_p)$.

If Φ is now a systems of eigenvalues, the previous implies that the associated semsimple representation

$$\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$$

can be realized on a finite extension of $\mathbf{F}_p$ depending only on N and p. If K_ρ is the field fixed by the kernel of ρ, then we see that the degree $[K_\rho : \mathbf{Q}]$ is bounded by a constant independent of the system Φ chosen. Since $K_\rho/\mathbf{Q}$ is unramified outside pN, by the Hermite-Minkowski theorem we see that there are only finitely many possibilities for K_ρ. □

The following more precise result has been shown by Tate, Serre, Jochnowitz for low levels (cf. [24], 4.1) and by Ash-Stevens for arbitrary N (cf. [1]).

Theorem 3.2.21. *Let Φ be a system of mod p Hecke eigenvalues arising from $\mathbf{M}(\Gamma_1(N), \overline{\mathbf{F}}_p)$. Then there exist integers k, h with $k \leq p+1$, and a system of Hecke eigenvalue Ψ arising from $\mathbf{M}_k(\Gamma_1(N), \overline{\mathbf{F}}_p)$ so that $\Phi = \Psi^{(h)}$.*

Yet a different proof of this theorem appears in [14], th 3.4. The question for a system of Hecke eigenvalues Φ to admit a *unique* twist to a system of weight k, where $2 \leq k \leq p+1$, is related to whether the associated representation ρ is tamely ramified at p, as we shall explain in the next section.

3.3 Modular mod p Galois representations

3.3.1 The local representation at p

Let p be a prime and N an integer not divisible by p. Let $f \in \mathbf{M}_k(\Gamma_1(N), \overline{\mathbf{F}}_p)$ be a mod p, normalized eigenform of type (k, ϵ) with eigenvalues a_ℓ, for ℓ prime, and assume that $2 \leq k \leq p+1$. Let

$$\rho_f : G_{\mathbf{Q}} \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$$

be the unique, semisimple Galois representation associated to f, we denote ρ_f simply by ρ, if this does not cause confusion. For f in this weight range, a great deal of information is known about the local shape at p of ρ thank to two theorems of Deligne and Fontaine (cf. [14]). These facts, joined with a theorem of Gross, allow us to give an answer to the question raised at the end of previous section of whether there might exist two distinct normalized eigenforms f and g whose weights are in the range $2, \ldots, p+1$ and so that the associated Galois representations satisfy $\rho_f \otimes \chi_p^h \simeq \rho_g$, for some power h of the mod p cyclotomic character χ_p.

Let $\mathfrak{p}$ be a prime of $\bar{\mathbf{Z}}$ above p and identify the corresponding decomposition subgroup $D_{\mathfrak{p}}$ of $G_{\mathbf{Q}}$ with $G_{\mathbf{Q}_p}$ =Gal($\bar{\mathbf{Q}}_p/\mathbf{Q}_p$). We denote the inertia subgroup $I_{\mathfrak{p}}$ simply by I. Let $\rho_p : G_{\mathbf{Q}_p} \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ denote the local representation at p obtained by restricting ρ to $G_{\mathbf{Q}_p}$.

Theorem 3.3.1. *(Deligne) Suppose that the eigenvalue $a_p \neq 0$. Then ρ_p is reducible and*

$$\rho_p \sim \begin{pmatrix} \chi_p^{k-1}\lambda(\epsilon(p)/a_p) & * \\ 0 & \lambda(a_p) \end{pmatrix}$$

Where χ_p is the mod p cyclotomic character and $\lambda(x)$ is the unique unramified character $\lambda : G_{\mathbf{Q}_p} \to \overline{\mathbf{F}}_p^*$ which sends Frob_p to $x \in \overline{\mathbf{F}}_p$.

If the characters $\chi_p^{p-1}\lambda(\epsilon(p)/a_p)$ and $\lambda(a_p)$ describing the semisimplification of ρ_p are distinct, then ρ_p is semisimple if and only if ρ_p is tamely ramified, that is the restriction $\rho_p|I$ of ρ_p to I factors through the tame inertia (cf. [49] 1.3). In this case, Gross proved the following criterion for ρ_p to be tamely ramified conjectured by Serre (cf. [17]).

Theorem 3.3.2. *(Gross) Let f be a normalized eigenform of type (k, ϵ) with $2 \leq k \leq p$. Suppose that $a_p \neq 0$ and that $\epsilon(p) \neq a_p^2$ if $k = p$. Assume further that ρ is irreducible. Then ρ is tamely ramified at p if and only there exists a normalized eigenform g of type $(p + 1 - k, \epsilon)$ so that $\theta(f) = \theta^k(g)$. The two Galois representations ρ_f and ρ_g satisfy $\rho_f \otimes \chi_p^{k-1} \simeq \rho_g$. Equivalently, a twist $\rho \otimes \chi_p^h$ of ρ, with $0 < h < p - 1$, arises from a cuspidal eigenform of weight k' with $1 \leq k' \leq p - 1$ if and only if ρ is tamely ramified.*

Notice that in the statement of theorem the possibility for the weight k of f to be $p + 1$ is neglected. This is because, by a theorem of Mazur (cf. [14]), if the filtration of $w(f)$ of f is equal to $= p+1$ and the representation ρ is irreducible, then ρ_p is *not* tamely ramified, and therefore not semisimple.

The two forms (f, g) of the theorem, when they exist, are called by Serre *companion forms*. A very special case occurs when f is self–companion, namely when $k = (p + 1)/2$ and $\rho_f \otimes \chi_p^{(p-1)/2} \simeq \rho_f$. In the next section we will examples of this phenomenon in the context of dihedral representations.

Let now ψ and ψ^p be the two fundamental characters $\psi, \psi^p : I \to \mathbf{F}_{p^2}^*$ of level 2 (cf. Serre, loc. cit. 1.7) . We have

Theorem 3.3.3. *(Fontaine) Let f be a normalized cuspidal eigenform of weight $k \leq p+1$. Suppose that the eigenvalue $a_p = 0$. Then ρ_p is irreducible and the restriction to the inertia subgroup satisfies*

$$\rho_p | I \sim \begin{pmatrix} \psi^{k-1} & 0 \\ 0 & \psi^{p(k-1)} \end{pmatrix}$$

In this case we call the system of eigenvalues arising from f a *supersingular* system. In particular if $a_p = 0$ then the representation $\rho_p|I$ factors through the tame quotient I^t (cf. Serre, 1.3 loc. cit.). In this case we have that $\theta^{p-1}(f) = f$, and from the analysis of the θ-cycle of f (cf. [23]) it follows that that the filtration $w(f)$ of f cannot be congruent to 1 mod p. Therefore we must have $2 \leq k \leq p$. Moreover, if $k > 2$ then we have that the form $g = \theta^{p+1-k}(f)$ has filtration $k' = p + 3 - k$ and the representations ρ_f and ρ_g satisfy $\rho_f \otimes \chi_p^{p+1-k} \simeq \rho_g$.

3.3.2 The dihedral case

Let $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ be a continuous representation. We will say that ρ is of *dihedral type* if ρ is irreducible and the projective image of ρ in $\mathrm{PGL}_2(\overline{\mathbf{F}}_p)$ is isomorphic to a dihedral group.

The modularity of *odd* representations ρ of dihedral type was known long time before Serre's conjecture was proved, at least for $p > 2$. The reason is perhaps because, if $p > 2$, any mod p representation ρ of dihedral type has a characteristic zero realization

$$\tilde{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathcal{O}),$$

where $\mathcal{O}$ is the ring of integers of a number field. What we mean is that there exists a prime $\mathfrak{p}$ of $\tilde{\rho}$ of residual characteristic p so that the reduction $\tilde{\rho}$ mod $\mathfrak{p}$ is isomorphic to ρ. We may even choose $\tilde{\rho}$ to have image isomorphic to that of ρ.

By a theorem of Weil-Langlands, the Artin L-function $L(s, \tilde{\rho})$ associated to $\tilde{\rho}$ (cf. [36]) coincides with the Dirichlet series of a cuspidal, normalized newform f on $\Gamma_0(N)$ of type $(1, \epsilon)$, where ϵ is the determinant of $\tilde{\rho}$ and N is the conductor of ϵ (cf [50] 3, 7).

The reduction mod p of f is a cuspidal, mod p eigenform whose associated eigensystem $\Phi = (a_\ell)$ is so that $a_\ell = \mathrm{tr}(\rho(\mathrm{Frob}_\ell))$, and the modularity of ρ follows. It is curios to observe that the (modified) Serre's weight attached to ρ is not 1, in general. However here the prime p is allowed in the level N of f, whereas Serre's weight is minimal among all the weights of mod p modular forms f that give rise to ρ and whose level is *prime* to p.

Even though dihedral representations are very well understood, our modest goal is to point out how some of them provide examples of systems of eigenforms that are self–companion and how others give examples of systems of eigenvalues that are supersingular. We will assume that $p > 2$.

We first recall some generalities on representations of dihedral type (cf. [50] 7). Let $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ be a continuous representation of *dihedral type*. The $\bar{\rho}$ be the projective image of ρ in $\mathrm{PGL}_2(\overline{\mathbf{F}}_p)$ is then isomorphic to the dihedral group D_n, for a certain integer $n \geq 2$. Recall that $D_n \simeq C_n \rtimes \mathbf{Z}/2$ is the semidirect product between a cyclic normal subgroup C_n of order n and the group generated by an involution, acting on C_n by $x \to x^{-1}$. If $n \geq 3$, then C_n is uniquely determined.

Consider the character $\omega : G_{\mathbf{Q}} \to D_n/C_n = \{\pm 1\}$ obtained by composing $\bar{\rho}$ with the projection $D_n \to D_n/C_n$. The character ω corresponds to a quadratic field K, uniquely determined if $n \geq 3$.

Lemma 3.3.4. *Let $\rho : G_{\mathbf{Q}} \to GL_2(\overline{\mathbf{F}}_p)$ be a two–dimensional, dihedral, mod p representation of $G_{\mathbf{Q}}$, assume that $p > 2$. Then, the group $Im(\rho)$ consists of semisimple elements of $GL_2(\overline{\mathbf{F}}_p)$.*

Proof. Choose a cyclic subgroup C_n of order n of $D_n = \mathrm{Im}(\bar{\rho})$ and let $\tau \in \mathrm{PGL}_2(\overline{\mathbf{F}}_p)$ be a generator. We claim that the action of τ on $\mathrm{P}^1(\overline{\mathbf{F}}_p)$ has exactly two distinct fixed lines. Since τ is a nontrivial element, certainly the number of lines fixed by τ do not exceed 2. On the other hand, if τ had precisely one fixed line r then the subgroup of $\mathrm{PGL}_2(\overline{\mathbf{F}}_p)$ that normalizes τ would be contained in the group stabilizing r. In particular, $\mathrm{Im}\bar{\rho}$ would stabilize r and ρ would be reducible. A contradiction. Therefore τ fixes precisely two distinct lines of $\mathrm{P}^1(\overline{\mathbf{F}}_p)$ and any lifting of an element of C_n is a semisimple element of $\mathrm{GL}_2(\overline{\mathbf{F}}_p)$. Assume now that $\sigma \in \mathrm{Im}(\rho)$ is an element whose image $\bar{\sigma}$ in $\mathrm{PGL}_2(\overline{\mathbf{F}}_p)$ does not belong to C_n. Then $\bar{\sigma}$ interchanges the two distinct lines fixed by τ and therefore σ will be conjugate to a matrix of the form

$$\begin{pmatrix} 0 & \beta \\ \gamma & 0 \end{pmatrix}, \tag{3.4}$$

and if $p \neq 2$ such a matrix has distinct eigenvalues in $\overline{\mathbf{F}}_p^*$. □

It follows from the lemma that the image of ρ has order prime to p and the restriction of ρ to $G_K = \mathrm{Gal}(\bar{K}/K)$ is abelian and completely reducible. Therefore let

$$\varphi, \varphi' : G_K \to \overline{\mathbf{F}}_p^*$$

be the two characters appearing in the decomposition of $\rho|G_K$. If $\sigma \in G_{\mathbf{Q}}$ with $\omega(\sigma) = -1$, denote by φ^σ the character of G_K defined by the formula $\varphi^\sigma(x) = \varphi(\sigma x \sigma^{-1})$. It follows that either $\varphi = \varphi^\sigma$ or $\varphi \neq \varphi^\sigma$ and $\varphi' = \varphi^\sigma$. Since ρ is assumed irreducible, the latter of the possibilities occurs. Moreover, we have that

$$\det \circ \rho = \omega \cdot \varphi_{\mathbf{Q}},$$

where $\varphi_{\mathbf{Q}}$ is the character of $G_{\mathbf{Q}}$ obtained by the composition $\varphi \circ \mathrm{ver}_{K/\mathbf{Q}}$, where $\mathrm{ver}_{K/\mathbf{Q}}$ is the transfer map (cf. [36]).

Lemma 3.3.5. *There is an isomorphism $\rho \simeq \rho \otimes \omega$.*

Proof. Since the image of ρ has order prime to p, one can show this by comparing the traces of the two representations in question. The statement is then reduced to show that $\mathrm{tr}(\sigma) = 0$ whenever $\omega(\sigma) = -1$. But if $\omega(\sigma) = -1$, then σ reduces to an order two element of $\mathrm{PGL}_2(\overline{\mathbf{F}}_p)$ that normalizes the cyclic subgroup C_n of $\mathrm{Im}(\bar{\rho})$, and, we have seen it, σ is conjugate to a matrix of the form 3.4. Therefore $\mathrm{tr}(\sigma) = 0$. □

Suppose now that ρ is furthermore an *odd* representation. We recall that associated to ρ there is the quadratic character

$$\omega : G_{\mathbf{Q}} \to \{\pm 1\},$$

obtained by composing $\bar{\rho}$ with the projection $D_n \to D_n/C_n$. Also, the quadratic field corresponding to ω is denoted by K.

Proposition 3.3.6. *Let p be an odd prime and f a cuspidal, mod p, normalized eigenform of type (k, ϵ), where $2 \leq k \leq p+1$, with system of eigenvalues $\Phi = (a_\ell)$, where ℓ is any prime. Assume that the associated mod p representation ρ_f is dihedral. Assume further, that, in the above notation, the field K may be taken to be the unique quadratic field ramified only at p, so that $\omega = \chi_p^{(p-1)/2}$ is the quadratic character of conductor p. Then*

i) if $a_p \neq 0$ then $k = (p+1)/2$ and f is self–companion;

ii) if $a_p = 0$ then $k = (p+3)/2$.

Moreover, let $\varphi : G_K \to \overline{\mathbf{F}}_p^*$ be the character of G_K so that $\rho_f \simeq Ind_K^{\mathbf{Q}}(\varphi)$. Then, the second possibility occurs if and only if φ is ramified at the place of K above p.

Proof. The representation ρ_f satisfies $\rho_f \simeq \rho_f \otimes \chi_p^{(p-1)/2}$ by lemma 3.3.5. Equivalently, we have $\theta(f) = \theta^{(p+1)/2}(f)$. Now if $a_p \neq 0$ this means that f is self–companion and

$k = p + 1 - k$, which implies $k = (p+1)/2$. Moreover, by the local description of ρ_f at a decomposition group at p, given by Theorem 3.3.1, we see that φ is unramified at the place of K above p.

On the other hand if $a_p = 0$ then this means that $\theta^{p-1}(f) = f$ and, by the classification of the possible θ-cycles of f, we have that the assumption $\theta(f) = \theta^{(p+1)/2}(f)$ implies that f has weight $(p+3)/2$. The local description of ρ_f at a decomposition group at p given by theorem 3.3.3 implies that φ is (tamely) ramified at the place of K above p. □

As an application, consider the case where $p \equiv 3 \bmod 4$. Let $K = \mathbf{Q}\sqrt{-p}$ be the unique quadratic field unramified outside p, and ω the associated quadratic character of $G_{\mathbf{Q}}$. Denote by $h(p)$ the class number of K.

Proposition 3.3.7. *There are precisely $(h(p)-1)/2$ distinct, normalized, mod p eigenforms of weight $(p+1)/2$ and level 1 that are self–companion. They correspond to pairs of distinct characters*

$$\varphi, \varphi' : Cl_K \to \overline{\mathbf{F}}_p^*$$

so that $\varphi = \varphi^{-1}$.

Proof. Consider the group A of characters

$$\varphi : G_K \to \overline{\mathbf{F}}_p^*$$

that are everywhere unramified. Since p does not divide the class number $h(p)$ of K (in fact $h(p) \leq (p-1)/2$, cf. [3] 5, §4, Thm. 4), we have that A may be identified with the Pontryagin dual Cl_K^* of the ideal class group Cl_K of K. The Galois group $G(K/\mathbf{Q})$ of the quadratic extension $K/\mathbf{Q}$ acts on Cl_K by the formula $\sigma \cdot \varphi(x) = \varphi(\sigma^{-1}x\sigma)$. Since the extension $K/\mathbf{Q}$ is totally ramified at p and unramified outside p, the subgroup of invariants

$$(\mathrm{Cl}_K^*)^{G(K/\mathbf{Q})}$$

is trivial (this fact follows from the fact that $\mathbf{Q}$ has class number one, cf [6] for details).

This implies that for $\sigma \in G_{\mathbf{Q}}$ with $\omega(\sigma) = -1$, we have $\varphi^\sigma \neq \varphi$ for any nontrivial $\varphi \in \mathrm{Cl}_K^*$. Also, it follows from the properties of the Artin symbol that $\varphi^\sigma = \varphi^{-1}$. In particular the class number $h(p)$ of K is odd.

Take now a nontrivial $\varphi \in \mathrm{Cl}_K^*$. From what we have just seen, we have that the two–dimensional representation $\rho = \mathrm{Ind}_K^{\mathbf{Q}}(\varphi)$ is irreducible, of dihedral type (in fact $\mathrm{Im}\rho$ is dihedral) and its isomorphism class is unchanged if we replace σ by σ^{-1}.

Let now $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ be a matrix realization of ρ. Since the $\varphi^\sigma = \varphi^{-1}$ for σ so that $\omega(\sigma) = -1$, it is easy to see that the determinant of ρ is $\omega = \chi_p^{(p-1)/2}$, and therefore odd, since $p \equiv 3 \bmod 4$.

The Serre's invariants N and k of ρ are respectively 1 and $(p+1)/2$. Therefore it follows from Serre's conjecture that there exist a normalized cuspidal eigenform f of weight $(p+1)/2$ so that $\rho \simeq \rho_f$, where ρ_f is the mod p representation attached to f (alternatively, one may deduce that the weight of f must be $(p+1)/2$ from proposition 3.3.6). From proposition 3.3.6 we see that f is the self–companion form of weight $(p+1)/2$ and level 1 attached to the unordered pair φ, φ^{-1}.

In the other direction, assume that f is a self–companion, normalized, mod p, cuspidal eigenform of weight (necessarily) equal to $(p+1)/2$. Let $\Phi = (a_\ell)$ be the associated system of Hecke eigenvalues and let ρ_f be the associated odd, mod p representation of $G_{\mathbf{Q}}$. Then ρ_f is unramified outside p and its determinant is ω, the quadratic character corresponding to K. Since f is self–companion, we have $\rho_f \simeq \rho_f \otimes \omega$.

We show that ρ_f has dihedral image. Let G be the image of ρ_f and H the intersection between G and $\mathrm{SL}_2(\overline{\mathbf{F}}_p)$. We have that H in normal with index two in G, since $\det \circ \rho$ is a quadratic character. Let now $\ell \neq p$ be so that $\omega(\mathrm{Frob}_\ell) = -1$, for a choice Frob_ℓ of a Frobenius element at ℓ. We have that $\rho(\mathrm{Frob}_\ell) \notin H$ and its characteristic polynomial is

$$X^2 - a_\ell X - 1.$$

The isomorphism $\rho_f \simeq \rho_f \otimes \omega$ now implies that, for such choice of ℓ, the trace a_ℓ must be zero. In particular, $\rho(\mathrm{Frob}_\ell)$ has order two. Since any element $\sigma \in G - H$ is equal $\rho(\mathrm{Frob}_\ell)$ for an appropriate choice of ℓ, we have that all the elements lying in the H-coset $G - H$ have order two. This immediately implies that H is abelian. Let in fact $\sigma \in G - H$ be any element. We have that σh has order two for all $h \in H$ since it belongs to the coset $G - H$. Therefore $\sigma h \sigma h = 1$ for all $h = in H$. Equivalently, $\sigma h \sigma = h^{-1}$ for all $h \in H$. But σ has order two and the previous equation may be written as $\sigma h \sigma^{-1} = h^{-1}$, from which we can conclude that the automorphism given by conjugation by σ on h coincides with the inversion map $h \to h^{-1}$. In particular, the inversion map is an automorphism and hence H is abelian.

The group H is the Galois group of an unramified extension of K and, since $p \nmid h(p)$ as already remarked, the action of H on the two–dimensional vector space of ρ_f is completely reducible and decomposes as the sum of two characters φ and φ' of Cl_K, valued in $\overline{\mathbf{F}}_p$.

We see now that $\varphi = \sigma \cdot \varphi'$, for any $\sigma \in G_{\mathbf{Q}}$ such that $\omega(\sigma) = -1$, and therefore the two characters are inverses of each other, H is cyclic and $\rho \simeq \mathrm{Ind}_K^Q(\varphi)$. □

3.4 Modular forms mod p and quaternions

3.4.1 Supersingular elliptic curves

Let $\Phi : \mathrm{Spec}(\overline{\mathbf{F}}_p) \to \mathrm{Spec}(\overline{\mathbf{F}}_p)$ be the Frobenius morphism, and view $\mathrm{Spec}(\overline{\mathbf{F}}_p)$ as a scheme above itself via Φ. If X is any scheme above $\overline{\mathbf{F}}_p$, with structure morphism $\pi_X : X \to \overline{\mathbf{F}}_p$, denote by $X^{(p)}$ the scheme over $\overline{\mathbf{F}}_p$ obtained as the fiber product between Φ and π_X. The diagram

$$\begin{array}{ccc} X & \xleftarrow{\Phi_X} & X^{(p)} \\ {\scriptstyle \pi_X}\downarrow & & \downarrow{\scriptstyle p_X} \\ \mathrm{Spec}(\overline{\mathbf{F}}_p) & \xleftarrow{\Phi} & \mathrm{Spec}(\overline{\mathbf{F}}_p) \end{array}$$

is cartesian, the structure morphism of $X^{(p)}$ is $\Phi \circ \mathfrak{p}_X = \pi_{X^{(p)}}$.

Let now $E/\overline{\mathbf{F}}_p$ be an elliptic curve over $\overline{\mathbf{F}}_p$. Denote by $A \in \underline{\omega}_E^{\otimes p-1}$ the Hasse invariant. The standard construction above applied to E, gives an elliptic curve $E^{(p)}$ over $\overline{\mathbf{F}}_p$ with an inseparable degree p isogeny $\Phi_E : E^{(p)} \to E$ (cf. [54],II,prop.2.11). Let $\hat{\Phi}_E : E \to E^{(p)}$ be the dual isogeny of Φ_E (cf. Silverman, loc.cit. III, §6). It is a classical result of Deuring that

Proposition 3.4.1. *The following conditions are equivalent*

i) $E[p](Spec(\overline{\mathbf{F}}_p)) = 0$*;*

ii) $\hat{\Phi}_E$ *is inseparable;*

iii) $End_{\overline{\mathbf{F}}_p}(E)$ *is a maximal order in a quaternion algebra;*

iv) the Hasse invariant A *is zero.*

(cf. Silverman, loc.cit. V, th.3.1)

If E satisfies the equivalent conditions of the proposition, then E is called a *supersingular* elliptic curves. Its j-invariant $j(E)$ belongs to $\mathbf{F}_{p^2}$. Consider in fact the degree p, (purely) inseparable isogeny $\hat{\Phi}_E : E \to E^{(p)}$. There exists a morphism Ψ so that $\hat{\Phi}_E$ factors as

$$E \xrightarrow{\Psi} E^{(p^2)} \xrightarrow{\Phi_{E^{(p)}}} E^{(p)}$$

(cf. [20] IV, prop. 2.5), where $\Phi_{E^{(p)}}$ is the Frobenius isogeny associated to $E^{(p)}$, and $E^{(p^2)}$ denotes $(E^{(p)})^{(p)}$. Comparing degrees, we see that Ψ has degree one, and therefore it is an automorphism.

Lemma 3.4.2. *Let E be a super singular elliptic curve. Then there exists an elliptic curve E^0 defined over $\mathbf{F}_{p^2}$ so that*

i) $E^0 \otimes \overline{\mathbf{F}}_p \simeq E$;

ii) the $\mathbf{F}_{p^2}$ Frobenius $\Phi^2_{E^0} : E^0 \to (E^0)^{p^2} = E^0$ equals $-p$ in End$(E^0 \otimes \overline{\mathbf{F}}_p)$;

iii) all the $\overline{\mathbf{F}}_p$-endomorphisms of E^0 are defined over $\mathbf{F}_{p^2}$.

Moreover, E^0 is unique up to $\mathbf{F}_{p^2}$-isomorphism.

Proof. The existence of E^0 satisfying i) follows from the existence of Ψ above. The fact that the model E^0 over $\mathbf{F}_{p^2}$ can be chosen in such a way ii) holds is proved in [19]. Part iii) follows from Tate-Honda theory ([56], Théorème 1), the last assertion follows from iii). □

In particular, there are only finitely many isomorphism classes of supersingular elliptic curves E over $\overline{\mathbf{F}}_p$. Given the existence of E^0 as in the lemma, an important consequence of Tate–Honda theory is that supersingular elliptic curves form a single isogeny class (cf. Tate, loc. cit.).

3.4.2 Quaternion algebras

In this section we introduce some notation, recall the structure theorem for quaternion algebras over a global field, and give the construction of the unique quaternion, division algebra over $\mathbf{Q}_p$. We refer to [57] for the details and for the proofs.

Let K be any field, and H a finite dimensional, associative K-algebra with identity. The fact that $1 \in H$ allows us to identify K with a central subring of H.

Definition 3.4.3. H is a *quaternion* algebra over K if it is simple, of dimension four, and its center coincides with K.

An example of a quaternion algebra H over K is provided by the algebra $M_2(K)$ of two by two matrices with coefficients in K. Any quaternion algebra H over K that is not isomorphic to $M_2(K)$ is a *division* algebra (*corps*) (cf. Vignéras, loc. cit.). If K is separably closed then any H is isomorphic to $M_2(K)$.

Let K be a global field and ν a place of K, then a quaternion algebra H over K defines a quaternion algebra H_ν over the completion K_ν of K at ν by

$$H_\nu = K_\nu \otimes_K H.$$

We will say that H is *split* at ν if $H_\nu \simeq M_2(K_\nu)$, and that H is *ramified* at ν if H_ν is a division algebra. There is the following classification theorem (cf. Vignéras, loc. cit., III, §3)

Theorem 3.4.4. *Let H be a quaternion algebra over a global field K, then the set S of places of K where H ramifies is finite, of even cardinality and uniquely determines H, up to isomorphism. For any finite set S of places of K of even cardinality there exists a quaternion algebra H ramified precisely at the places in S.*

In order to define a quaternion algebra D over a global field K, it therefore suffices to prescribe the finite set of places where D ramifies, which has to be of even cardinality.

Assume now that K is a local field of characteristic zero. If $K\mathbf{R}$, we have (cf. Vignéras, loc. cit., I, §2)

Theorem 3.4.5. *(Frobenius) Let H be a quaternion algebra over $\mathbf{R}$. If H is a division algebra, then H is isomorphic to the algebra of Hamiltonian quaternions, otherwise $H \simeq M_2(\mathbf{R})$.*

In the nonarchimedean case we have (cf. Vignéras, loc. cit.,II)

Theorem 3.4.6. *Let K be a finite extension of $\mathbf{Q}_p$. Then, up to isomorphism, there exist only one quaternion, division algebra over K.*

There is an explicit construction of the unique quaternion, division algebra over a p-adic field K that we shall describe for $K = \mathbf{Q}_p$, the general case being analogous.

In what follows an *order* of a quaternion algebra H over $\mathbf{Q}_p$ consists of a subring R of H containing $\mathbf{Z}_p$, of finite type over $\mathbf{Z}_p$, and so that R is a $\mathbf{Z}_p$-lattice in H, that is $R\mathbf{Q}_p = H$. In the next section the definition of order will be extended to a more general setting.

Let $L/\mathbf{Q}_p$ be the unique unramified, quadratic extension of $\mathbf{Q}_p$, denote by O_L the ring of integers of L and by P_L the maximal ideal of O_L. If $x \in L$ then $\bar{x}$ denotes its Galois conjugate over $\mathbf{Q}_p$.

Consider now a two–dimensional vector space H over L and set $H = L \oplus L\pi$, where $\{1, \pi\}$ is a basis for H. Define on H the associative multiplication that extends the multiplication on L, and so that

$$\pi x = \bar{x}\pi \ \ \textit{and} \ \ \pi^2 = p \in L, \ \ \text{for all } x \in L.$$

For $x, y, v, w \in L$, the multiplication on H is then defined by

$$(x + y\pi)(v + w\pi) = xv + y\bar{w}p + (xw + y\bar{v})\pi.$$

The center of H is $\mathbf{Q}_p$ and it is easy to see that H is simple. Define the $\mathbf{Q}_p$-linear anti-involution σ of H (meaning that $\sigma(hh') = \sigma(h')\sigma(h)$) by the formula

$$\sigma(x + y\pi) = \overline{x + y\pi} = \bar{x} - y\pi,$$

where $x, y \in L$. The involution σ extends Galois conjugation on L, and $\mathbf{Q}_p$ consists of the subspace of fixed points of σ. The *reduced trace* tr and *reduced norm* N on H are defined by

$$\mathrm{tr}(\alpha) = \alpha + \bar{\alpha}, \quad N(\alpha) = \alpha\bar{\alpha}.$$

The trace is additive, the norm is multiplicative and they are both valued in $\mathbf{Q}_p$. Explicitly, $\alpha = x + y\pi$, with $x, y \in L$, then $\mathrm{tr}(\alpha) = x + \bar{x}$ and $N(\alpha) = x\bar{x} - y\bar{y}p$.

Let ν_p denote the additive valuation on $\mathbf{Q}_p$, normalized so that $\nu_p(p) = 1$. Then $\nu_p(x\bar{x})$ is even and $\nu_p(-y\bar{y}p)$ is odd, therefore $N(\alpha) = 0$ only if $\alpha = 0$ in H. It follows that H is a division algebra.

The algebra H act on itself by right multiplication, for $h \in H$, let

$$r_h : H \longrightarrow H$$

be the map defined by $r_h(x) = xh$. Since H is associative, we see that r_h is L-linear and any element $h \in H$ can be identified with a two by two matrix with entries in L. Explicitly, in the coordinates given by the basis $\{1, \pi\}$, we have that if $h = x + y\pi$, with $x, y \in L$, then

$$r_h \sim \begin{pmatrix} x & \bar{y}p \\ y & \bar{x} \end{pmatrix}.$$

However, the map $H \ni h \to r_h \in M_2(L)$ is not a $\mathbf{Q}_p$-algebras homomorphism since $r_h r_{h'} = r_{h'h}$ and it is preferable to apply an anti-involution of $M_2(L)$ to obtain an embedding of H is the former. If we choose the involution to be transposition, we see that $h \in H$ may be identified with the matrix

$$r_h^t \sim \begin{pmatrix} x & y \\ \bar{y}p & \bar{x} \end{pmatrix}.$$

The map $h \to r_h^t$ exhibits an isomorphism between H and the algebra of matrices of the above type. In particular, h satisfies the polynomial

$$T^2 - \mathrm{tr}(h)T + N(h),$$

which has $\mathbf{Q}_p$ coefficients. If $h \neq 0$, then $h^{-1} = N(h)^{-1}(\mathrm{tr}(h) - h)$.

Remark 3.4.7. The construction just described can be carried out in a the analogous way when $\mathbf{Q}_p = \mathbf{R}$, by setting $L = \mathbf{C}$. The algebra H obtained, gives the classical Hamiltonian quaternions.

An element $h \in H$ is integral over $\mathbf{Z}_p$ (cf. 3.4.3 for the definition) if and only if $\mathrm{tr}(h) \in \mathbf{Z}_p$ and $N(h) \in \mathbf{Z}_p$. These two conditions imply that h in integral over $\mathbf{Z}_p$ if and only if $h = a + b\pi$, where $a, b \in O_L$. The set of integral elements form therefore a subring $R_H = O_L + O_L\pi$ of H, which is the unique *maximal order* of H (cf. 3.4.3).

There is an additive valuation ν_H on H defined by

$$\nu_H(h) = \nu_p(N(h)),$$

the ring R_H coincides with the valuation ring of ν_H, that is $R_H = \{h \in H | \nu_H(h) \geq 0\}$. If R_H^* is the unit group of R_H, it follows from the existence of ν_H that the elements of strictly positive valuation

$$P_H = \{h \in H | \nu_H(h) > 0\}$$

form the unique maximal ideal of R_H. We have $P_H = pO_L + O_L\pi$ and $P_H = (\pi)$, the principal ideal generated by π. Any element of valuation one is called a *uniformizer* of R_H, or of H.

The residue field R_H/P_H is isomorphic to O_L/P_L, a quadratic extension of $\mathbf{F}_p$. The units of R_H are the group $O_L^* + O_L\pi$, where O_L^* denotes the units of O_L. There is an exact sequence

$$0 \to R_H^+(1) \to R_H^* \to \mathbf{F}_{p^2}^* \to 0,$$

where $R_H^+(1)$ is the subgroup of units which are congruent to 1 (mod π), that is

$$R_H^+(1) = O_L^*(1) + O_L\pi = 1 + \pi R_H.$$

$R_H^+(1)$ is the maximal pro-p subgroup of R_H^*. The quotient $R_H^+/R_H^+(1)$ is isomorphic to the units of the residue field, we have $R_H^+/R_H^+(1) \simeq \mathbf{F}_{p^2}^*$.

3.4.3 Orders and ideals of quaternion algebras

We recall the notions of *order* and *ideal* for quaternion algebras over $\mathbf{Q}$ and $\mathbf{Q}_\ell$, where ℓ is a prime. We unify the exposition by working with a Dedekind domain A that, for our purposes, it is either $\mathbf{Z}$ or $\mathbf{Z}_\ell$. We then explain how the adelic language can be used to describe *ideal classes* of a quaternion algebra over $\mathbf{Q}$. For more details, we refer to [57].

Let A be a Dedekind domain (cf. [52], I, §3), K its field of fractions and H a quaternion algebra over K.

Definition 3.4.8. An A-submodule I of H is an *A-lattice* if it is finitely generated as A-module and if it contains a K-basis of H, that is $KI = H$. An element $x \in D$ is an *A-integer*, or is integral over A, if the A-subring of H generated by x, and denoted by $A[x]$, is a finitely generated A-module. An *A-order* R of H is a subring (containing 1) that is an A-lattice of H.

Any element x of an order R is an A-integer, since $A[x]$ is contained in the finitely generated A-module R, and A is noetherian and therefore $A[x]$ is also finitely generated. Orders exist since, for example, if $I \subset H$ is any A-lattice, then the ring

$$R(I) = \{x \in H | xI \subset I\}$$

is an order (cf. [57], p.20). Any subring R of H containing A, consisting of integers and which is an A-lattice is an order. From this characterization one can deduce that maximal orders exist (cf. Vignéras, loc. cit. p.20). All these notions clearly depend on the Dedekind domain A. However, in what follows the ring A will not always be specified since it will be implicit from the type of object considered.

Let now R be a fixed maximal order of H,

Definition 3.4.9. A *right ideal* I of R is an A-lattice of H that is stable under right multiplication by R.

We will simply refer to I as an ideal of R.
The product IJ of two ideals I and J of R is defined to be set of finite sums of products of elements of I and J. It is also a left ideal of R and multiplication between ideals of R is associative. Two ideals I and J are said *equivalent*, or to belong to the same class, if there exists $h \in H^*$ so that $hI = J$.

Proposition 3.4.10. *Let $A = \mathbf{Z}_\ell$ for a prime ℓ, H_ℓ be a quaternion algebra over $\mathbf{Q}_\ell$ and R_ℓ a maximal order of H_ℓ. Then every ideal of R_ℓ is principal.*

Proof. (Sketch) If H_ℓ is the division algebra over $\mathbf{Q}_\ell$, then the proposition follows from the existence of the additive valuation ν_{H_ℓ}, described in 3.4.2. In the case $H_\ell \simeq$, the proposition can be shown using the the theory of elementary divisors (for more details, cf. Vignéras, loc. cit.,II) □

A corollary of the proposition is that a local ideal I_ℓ of H_ℓ is given by $I_\ell = g_\ell R_\ell$, for some $g_\ell \in H_\ell^*$ (g_ℓ needs to be invertible for I_ℓ to be a lattice). Therefore ideals of H_ℓ are described by the coset space H_ℓ^*/R_ℓ^*.

Let $A = \mathbf{Z}$, and let $H_\mathbf{Q}$ be a quaternion algebra over $\mathbf{Q}$ with maximal order $R_\mathbf{Z}$.

Theorem 3.4.11. *The number n of ideal classes of $R_\mathbf{Z}$ is finite and depends only on $H_\mathbf{Q}$.*

(cf. Vignéras, loc. cit., III, Th 5.4)

Set $H_\ell = H_\mathbf{Q} \otimes_\mathbf{Q} \mathbf{Q}_\ell$ and $R_\ell = R_\mathbf{Z} \otimes_\mathbf{Z} \mathbf{Z}_\ell$, then R_ℓ is a maximal order of H_ℓ. Let I be an ideal of $R_\mathbf{Z}$ and, for a prime ℓ, set $I_\ell = I \otimes R_\ell$. We have that $I_\ell = R_\ell$ for almost all primes ℓ.

Proposition 3.4.12. *There is a correspondence between ideals I of $R_\mathbf{Z}$ and collections of local ideals (I_ℓ), indexed by primes ℓ, so that $I_\ell = R_\ell$ for almost all ℓ.*

(cf. Vignéras, loc. cit., III, prop. 5.1)

A corollary of the proposition is the adelic dictionary for ideal classes of $H_\mathbf{Q}$. Let $\mathbf{A}$ be the adéle ring of $\mathbf{Q}$ and $H_\mathbf{A} = \mathbf{A} \otimes_\mathbf{Q} H_\mathbf{Q}$ be the adéle ring of $H_\mathbf{Q}$. Let $H_\mathbf{A}^*$ denote the multiplicative group of $H_\mathbf{A}$, let $\hat{R} = R \otimes_\mathbf{Z} \hat{\mathbf{Z}} = \Pi_\ell R_\ell$ be the product of all the R_ℓ's with unit group $\hat{R}^* = \Pi_\ell R_\ell^*$. Let $H_\mathbf{R} = H_\mathbf{Q} \otimes \mathbf{R}$ be the component of $H_\mathbf{A}$ at infinity, with unit group $H_\mathbf{R}^*$. Then

Corollary 3.4.13. *The set of classes of right R-ideals of H is in bijection with the double coset*

$$H_\mathbf{Q}^* \backslash H_\mathbf{A}^* / \hat{R}^* \times H_\mathbf{R}^*$$

If I is an ideal, then for any prime ℓ we have $I_\ell = (g_\ell)$, for some $g_\ell \in H_\ell^*$. The adelic element $g = (\ldots, g_\ell, \ldots, 1) \in H_\mathbf{A}^*$ with (say) trivial component at infinity defines

the coset $g \cdot \hat{R}^* \times H_{\mathbf{R}}^*$. On the other hand, given any coset $g \cdot \hat{R}^* \times H_{\mathbf{R}}^*$ we have that $g\hat{R} \times H_{\mathbf{R}} \cap H$ defines the corresponding ideal of R.

3.4.4 Quaternion algebras and supersingular elliptic curves

Let D be the unique quaternion division algebra over $\mathbf{Q}$ ramified at $\{p, \infty\}$ (cf Th.3.4.4). We shall describe here the correspondence between left ideal classes of a maximal order of D and supersingular elliptic curves over $\overline{\mathbf{F}}_p$.

Let R be a maximal order of D and for any prime ℓ denote the corresponding local maximal order $R \otimes \mathbf{Z}_\ell$ by R_ℓ. If $\ell \neq p$, then the $\mathbf{Q}_\ell$ algebra $D_\ell = D \otimes \mathbf{Q}_\ell$ is isomorphic to the two by two matrix algebra $M_2(\mathbf{Q}_\ell)$, and we choose an isomorphism $D_\ell \simeq M_2(\mathbf{Q}_\ell)$ so that R_ℓ is identified with $\simeq M_2(\mathbf{Z}_\ell)$, the two by two matrix algebra with entries in $\mathbf{Z}_\ell$. The algebra D_p is isomorphic to the unique four dimensional division algebra over $\mathbf{Q}_p$ constructed in section 3.4.2, and R_p is its maximal order (D_p in 3.4.2 was denoted by H and R_p by R_H). The units of R_p are denoted by R_p^*, the units congruent to 1 modulo a uniformizer π of D_p by $R_p^*(1)$ (cf. 3.4.2). It is a classical theorem of Deuring that

Theorem 3.4.14. *There is a correspondence between isomorphism classes of supersingular elliptic curves E over $\overline{\mathbf{F}}_p$ and classes of right ideal of R in D.*

(cf. [18], §2, see below for the description of the correspondence)

The essential point in the theorem is that supersingular elliptic curves over $\overline{\mathbf{F}}_p$ describe a unique isogeny class. Let $\{E_i\}$, for $1 \leq i \leq n$, be a set of representatives for the isomorphism classes of supersingular elliptic curve so that the endomorphism ring of $E_1 = E$ is isomorphic to R. The set $I_i = \{\phi^{(i)} : E \to E_i\}$ of isogenies is a right R-ideal in $R \otimes \mathbf{Q} = D$ that uniquely determines E_i. Moreover, $E_i \simeq E_j$ if and only if there exists $g \in D^*$ so that $gI_i = I_j$. Let $\phi^{(i)} : E \to E_i$ be a nonzero isogeny, consider it as an element of $R \otimes \mathbf{Q} = D$. If $\ell \neq p$, then the local component $\phi_\ell^{(i)} \in D_\ell$ describes the associated morphism of ℓ-adic Tate modules $\phi_\ell^{(i)} : T_\ell(E) \to T_\ell(E_i)$. For $\ell = p$ the local component $\phi_p^{(i)} \in D_p$ describes the induced morphism $\phi_p^{(i)} : \mathcal{F}(E) \to \mathcal{F}(E_i)$, where $\mathcal{F}(E_i)$ is the formal group over $\overline{\mathbf{F}}_p$ associated to E_i (cf. [54] IV). Moreover, if $\omega \in E$ is an invariant differential defined over $\mathbf{F}_{p^2}$, then the corresponding differential ${\phi^{(i)}}_*\omega$ of E_i is uniquely determined by the image of $\phi_p^{(i)}$ in the coset $R_p^*(1)\backslash D_p^* = D_p^*/R_p^*(1)$ (cf. [19]).

Let now $N \geq 1$ be an integer prime to p. For any $\ell \neq p$ consider the subgroup $U_\ell(N)$ of $R_\ell^* = \mathrm{GL}_2(\mathbf{Z}_\ell)$ defined by

$$U_\ell(N) = \left\{ x \in \mathrm{GL}_2(\mathbf{Z}_\ell) | x \equiv \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \bmod \mathrm{N} \right\},$$

we have that $U_\ell(N) = R_\ell^*$ for every $\ell \nmid N$. At the prime p, set $U_p(1) = R_p^*(1)$ (cf. 3.4.2). Consider the product

$$U(1,N) = \Pi_{\ell \neq p} U_\ell(N) \times U_p(1) \times D_{\mathbf{R}}.$$

We have that $U(1,N)$ is a compact, open subgroup of $D_{\mathbf{A}}^*$ that contains the component at infinity. Thank to the identification of theorem 3.4.14, we can give an interpretation of the cosets space $D^* \backslash D_{\mathbf{A}} / U(1,N) \times D_{\mathbf{R}}^*$ in terms of enhanced supersingular elliptic curves.

Proposition 3.4.15. *There is a bijection between the double cosets space*

$$D^* \backslash D_{\mathbf{A}} / U(1,N) \times D_{\mathbf{R}}^*$$

and isomorphism classes of triples (E, α, ω), where E is a supersingular elliptic curve over $\overline{\mathbf{F}}_p$, α is a $\overline{\mathbf{F}}_p$-point of E of order N and ω is a nonzero differential on E that is defined over $\mathbf{F}_{p^2}$.

Proof. From corollary 3.4.13, classes of right ideal of R in D are in bijection with the space

$$D^* \backslash D_A / \hat{R}^* \times D_{\mathbf{R}}^*,$$

where $\hat{R}^* = \Pi_\ell R_\ell^*$ is the group of units of $\Pi_\ell R_\ell = R \otimes \hat{\mathbf{Z}}$. If $x \in D_{\mathbf{A}}$ denote by x_f the element of the finite adéles $\hat{D} = D \otimes_{\mathbf{Q}} \mathbf{A}^f$ obtained from x by disregarding the component at infinity. Let E be a supersingular elliptic curve so that $\mathrm{End}(E) = R$, let α be a point of E order N and ω a nonzero invariant form on E that is defined over $\mathbf{F}_{p^2}$. Let $D^* \cdot g \cdot U(1,N)$ be any element of the double coset $D^* \backslash D_{\mathbf{A}}^* / U(1,N)$. The right ideal $I_g = g\hat{R} \cap D$ is equipped with the additional structure of a point of order N of $I_g / N I_g$ and with a basis vector of $I_g / \pi I_g$. Choose a representative g of $D^* \cdot g \cdot U(1,N)$ so that the inverse I_g is integral, that is $\phi_\ell \in R_\ell$ for all primes ℓ, and all $\phi \in I_g$. Then any nonzero element ϕ of I_g defines an isogeny $\phi : E \to E$ of E into itself. The quotient of E by the intersection of the kernels of ϕ as ϕ ranges through all the elements of I_g is a supersingular elliptic curve E_g enabled with an invariant differential ω_g defined over $\mathbf{F}_{p^2}$ and a point α_g of order N. In this way we have described the correspondence. □

3.4.5 Restricting forms to the supersingular locus

In this section we explain a theorem that Serre sketched in a letter to Tate dated August 7th, 1987 (cf. [51]), relating systems of Hecke eigenvalues coming from mod p modular forms to those coming from locally constant functions on the adelic group $D^*_{\mathbf{A}}$, where D^* is the multiplicative group of the quaternion algebra ramified at $\{p, \infty\}$.

Let p be a prime and $N > 4$ a fixed integer prime to p. Let $X_1 = X_1(N)_{\overline{\mathbf{F}}_p}$ be the modular curve over $\overline{\mathbf{F}}_p$ introduced in proposition 1.1.15, and recall that the space $\mathbf{M}_k$ of mod p modular forms of weight k for $\Gamma_1(N)$ is identified with the sections of the invertible sheaf

$$\underline{\omega}_{\mathcal{E}}^{\otimes k} \otimes_{\mathbf{Z}[1/N]} \overline{\mathbf{F}}_p$$

on X_1, which will be denoted it by $\mathcal{M}_k$ for simplicity. The Hasse invariant A is a global section of $\mathcal{M}_{p-1}$, described by a modular form of level one. For any integer k, multiplication by A gives an exact sequence

$$0 \longrightarrow \mathcal{M}_{k-p+1} \longrightarrow \mathcal{M}_k \longrightarrow \mathcal{S}_k \longrightarrow 0 \tag{3.5}$$

where, by definition, $\mathcal{S}_k$ is the cokernel of multiplication by A. Since A has only simple zeros occurring precisely at the supersingular elliptic curves, the structure of $\mathcal{S}_k$ is easy to describe: it is zero outside the supersingular locus and one–dimensional over every supersingular elliptic curve.

Let then $\Sigma(N)$ be the set of isomorphism classes of pairs (E, α) where E is a supersingular elliptic curve over $\overline{\mathbf{F}}_p$ and $\alpha : \mu_N \to E[N]$ an embedding of $\overline{\mathbf{F}}_p$-group schemes. Every object (E, α) has no nontrivial automorphisms, thanks to the assumption $N > 4$. Moreover the datum of α is equivalent to that of an order N point of E, since $\mu_N \simeq \mathbf{Z}/N\mathbf{Z}$ over $\overline{\mathbf{F}}_p$. It follows that the cardinality of $\Sigma(N)$ is the number of isomorphisms classes of supersingular elliptic curves multiplied by the number of points of order N in $(\mathbf{Z}/N\mathbf{Z})^2$.

For $x = (E, \alpha) \in \Sigma(N)$, the stalk $\mathcal{S}_{k,x}$ of $\mathcal{S}_k$ at x is the one–dimensional space of invariant forms of weight k on E, given by elements of $\underline{\omega}_E^{\otimes k}$. The space S_k of global sections of $\mathcal{S}_k$ is therefore given by the sections of the natural map

$$\Pi_{x \in \Sigma(N)} \mathcal{S}_{k,x} \to \Sigma(N).$$

In other words elements $\gamma \in S_k$ are functions f that associates to every $x \in \Sigma(N)$ an invariant k-form $f(x)$ on E, where $x = (E, \alpha)$. The dimension of the space S_k equals the cardinality of $\Sigma(N)$.

The long exact cohomology sequence of 3.5 yields

$$0 \longrightarrow \mathbf{M}_{k-p+1} \longrightarrow \mathbf{M}_k \longrightarrow S_k \longrightarrow H^1(\mathcal{M}_{k-p+1}). \tag{3.6}$$

By Serre's duality, there is an isomorphism $H^1(\mathcal{M}_h) \simeq \text{dual}(H^0(\mathcal{M}_{-h} \otimes \Omega^1))$, since $\Omega^1 \simeq \mathcal{M}_2(-(cusps))$ ([17], 2, prop. 2.3). We have that, for all h,

$$H^1(\mathcal{M}_h) \simeq \text{dual}(\mathbf{M}^0_{2-h}).$$

In particular, $H^1(\mathcal{M}_h)$ is trivial for $h \geq 2$, and if $k \geq p+1$ the sequence

$$0 \longrightarrow \mathbf{M}_k \longrightarrow \mathbf{M}_{k-p+1} \longrightarrow S_k \longrightarrow 0$$

is exact. The space obtained from $\mathbf{M}_k$ by taking the quotient by forms of lower filtration will be denoted by

$$W_k = \mathbf{M}_k / \mathbf{M}_{k-p+1},$$

it is a module over all the Hecke operators (cf. 3.2.2). From what we have just seen, the injection

$$0 \to W_k \to S_k$$

is an isomorphism for $k \geq p+1$.

Proposition 3.4.16. *The Hecke operators T_ℓ and U_q, for $p \nmid pN$ and $q|N$, act naturally on S_k. The injection $W_k \to \mathcal{S}_k$ is a morphism of Hecke modules.*

For the proof cf. [19] 2.5.

The space $\mathcal{S}_k$ can be described as follows. Consider the set $\Sigma_1(N)$ of isomorphism classes of triples (E, α, ω), where E and α are as above and $\omega \in \underline{\omega}_E$ is a nonzero, invariant differential on E. The notion of isomorphism of triples is the evident one.

Proposition 3.4.17. *The space S_k is identified with the space of functions*

$$\varphi : \Sigma_1(N) \to \overline{\mathbf{F}}_p$$

so that for every $\lambda \in \overline{\mathbf{F}}_p^*$ we have $\varphi(E, \alpha, \lambda\omega) = \lambda^{-k}\varphi(E, \alpha, \omega)$.

This is clear, the correspondence between the two spaces is expressed by the formula $\varphi(E, \alpha, \omega)\omega^k = f(E, \alpha)$.

Proposition 3.4.18. *The space S_k depends only on the class of k modulo $p^2 - 1$.*

Proof. We have seen that any supersingular elliptic curve E admits a canonical structure on $\mathbf{F}_{p^2}$ where the Frobenius endomorphism ϕ_E is equal to $-p$ in $\mathrm{End}(E)$. It follows that also ω_E and its tensor powers have a canonical $\mathbf{F}_{p^2}$ structure. The tensor $\omega_E^{p^2-1}$ has therefore a canonical basis that gives an identification $\omega_E^k \simeq \omega_E^{k+p^2+1}$ compatible with isogenies (cf. [51]). It follows that $S_k \simeq S_{k+p^2-1}$ and the isomorphism is compatible with the action of Hecke operators. □

Thank to the periodicity of the space S_k we have that

Proposition 3.4.19. *A Systems of Hecke eigenvalues arising from $\mathbf{M}_k$ appears also in $S_{k'}$, for some $k' \equiv k \ mod \ (p-1)$, and viceversa.*

The main consequence of this is that instead of considering systems of Hecke eigenvalues coming from the algebra of mod p modular forms, one might consider the Hecke module

$$S(N) = \oplus_{0 \leq k \leq p^2-1} S_k$$

that has a simple description thank to the correspondence given in proposition 3.4.15. Let D be the quaternion algebra over $\mathbf{Q}$ ramified at $\{p, \infty\}$, let $D^*_{\mathbf{A}}$ be the adelic multiplicative group of D and let $U(1, N)$ be as in section 3.4.4.

Proposition 3.4.20. *The space $S(N)$ is in bijection with the set of functions*

$$f : D^* \backslash D^*_{\mathbf{A}} / U(1, N) \to \overline{\mathbf{F}}_p.$$

The bijection is equivariant with respect to the Hecke action.

Proof. Let V be the $\overline{\mathbf{F}}_p$-vector space of functions

$$f : D^* \backslash D^*_{\mathbf{A}} / U(1, N) \to \overline{\mathbf{F}}_p.$$

The group R_p^* acts by left translation on elements of V, the subgroup $U_p(1)$ acts trivially and the action factors through the quotient $R_p^*/U_p(1) = \mathbf{F}_{p^2}^*$. Since the order of $\mathbf{F}_{p^2}^*$ is prime to p, we have a decomposition into $\mathbf{F}_{p^2}^*$ isotypical components

$$V = \oplus_\Psi V^\Psi,$$

where $\Psi : \mathbf{F}_{p^2}^* :\to \overline{\mathbf{F}}_p$ ranges though all the $\overline{\mathbf{F}}_p$-valued characters of $\mathbf{F}_{p^2}^*$. Observe that a function $f \in V^\Psi$ satisfies $f(gx_p) = \Psi(x_p)f(g)$, for all $x_p \in U_p$, where by abuse of notation we regarded Ψ as a character of U_p.

We know that the double coset $D^*\backslash D_{\mathbf{A}}^*/U(1,N)$ may be identified with triples of (E, α, ω), where E is a supersingular elliptic curve, α is a point of E of order N and ω is a nonzero, invariant form on E defined over $\mathbf{F}_{p^2}$. It follows that any function $f \in V^\Psi$ extends uniquely to a function F on $\Sigma_1(N)$ by the rule

$$F(E, \alpha, \omega) = F(E, \alpha, \lambda\omega_0) = \Psi(\lambda)f(E, \alpha, \omega_0),$$

where if ω is a nonzero form on E, ω_0 is a nonzero form of E defined over $\mathbf{F}_{p^2}$ and λ is any constant in $\overline{\mathbf{F}}_p^*$. This shows that $V^\Psi \simeq S_k$, where k is the class of an integer mod $p^2 - 1$ so that $\Psi(\lambda) = \lambda^{pk}$. The equivarancy statement with respect to the Hecke action is proved in [19]. □

Let us just remark that the Hecke action of the Hecke operator T_ℓ for $\ell \neq p$ on functions on $D^*\backslash D_{\mathbf{A}}^*/U(1,N)$ is as follows. Let $f : D^*\backslash D_{\mathbf{A}}^*/U(1,N) \to \overline{\mathbf{F}}_p$ be any function, and consider it as the product of its local components $f = \Pi_\ell f_\ell$, where ℓ ranges through all the primes of $\mathbf{Q}$, finite or infinite. We have that f_ℓ is the function $f_\ell : D_\ell^* \to \overline{\mathbf{F}}_p$ obtained by restricting f to D_ℓ^*. Let now

$$U_\ell(N)\begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix} U_\ell(N) = \alpha_i \cup_i U_\ell(N)\alpha_i$$

be the disjoint $U_\ell(N)$–left cosets decomposition. Define $f_\ell|T_\ell : D_\ell^* \to \overline{\mathbf{F}}_p$ by

$$f_\ell|T_\ell(g) = \Sigma f_\ell(g\alpha_i).$$

This operator is well defined as f is left invariant by $U_\ell(N)$. It coincides with the operator $\pi(\tilde{T}_\ell)$ defined in 2.2.5. The action of ℓ-th Hecke operator $f|T_\ell$ on f is the function on $D_{\mathbf{A}}^*$ whose r-th component coincides with that of f, and whose ℓ-th component is given by $f_\ell|T_\ell$.

From the proposition it follows that there is an isomorphism of Hecke modules $S_k \simeq S_{pk}$. In fact, let π_p be the adélic element of $D_{\mathbf{A}}^*$ whose components x_ℓ are 1, if $\ell \neq p$ and so that $x_p = \pi$, where π is a uniformizer of D_p. Then $\pi_p U(1,N)\pi_p^{-1} = U(1,N)$ since $\pi U_p(1)\pi^{-1} = U_p(1)$. Moreover $\pi R_p^*\pi^{-1} = R_p^*$, and the induced action on the units of the

residue field $R_p^*/U_p(1)$ is the Galois conjugation given by the Frobenius automorphism $x \to x^p$. It follows that the map

$$V^{\Psi} \ni f \longrightarrow \pi \cdot f \in V^{\Psi^p} \tag{3.7}$$

where $\pi_p \cdot f(g) = f(\pi_p^{-1} g)$, described an isomorphism from V^{Ψ} to V^{Ψ^p}, therefore $S_k \simeq S_{pk}$. The isomorphism 3.7 intervenes only on the local component at p of functions on V^{Ψ}. Therefore it intertwines the action of every Hecke operator T_ℓ.

CHAPTER 4

A CONJECTURAL MASS FORMULA FOR CERTAIN MOD P REPRESENTATIONS OF $G_{\mathbf{Q}}$

4.1 A conjectural formula

4.1.1 The formula

Let $\mathbf{N}$ denote the set of integers > 0. A function f on $\mathbf{N}$ is said multiplicative if $f(1) = 1$ and $f(mn) = f(m)f(n)$, whenever m and n are coprime integers.

Let ℓ be any prime number, let r be multiplicative function defined by

$r(\ell) = \ell^2 - 3$;

$r(\ell^2) = \ell^4 - 3\ell^2 + 3$;

$r(\ell^n) = \ell^{2(n-3)}(\ell^2 - 1)^3$, for $n \geq 3$.

The order of growth of r with N is N^2.

Conjecture 4.1.1. *Let N be an integer ≥ 1 and p a prime number not dividing N. Let $R_N(p)$ be the number of isomorphism classes of odd, irreducible, two-dimensional Galois representations*

$$\rho : G_{\mathbf{Q}} \longrightarrow GL_2(\overline{\mathbf{F}}_p),$$

whose Serre's conductor equals N. Then $R_N(p)/(\frac{r(N)}{48}p^3) \to 1$ as $p \to \infty$, i.e. the order of growth of $R_N(p)$ with p is $\frac{r(N)}{48}p^3$.

4.1.2 Explanation of $r(N)$

The constant $r(N)/48$ has been obtained as follows. Let p be a prime number and $N \geq 1$ an integer not divisible by p. We will refer to a weight k so that $2 \leq k \leq p+1$ as to a *low weight*. Consider the space $\mathbf{M}_k^{0,+}(\Gamma_1(N))$ of cuspidal new form on $\Gamma_1(N)$ of

weight k. Using the exact formulas for the dimension of this space provided by ([35]) one sees that the sum

$$\sum_{2\leq k\leq p+1} \dim_{\mathbf{C}}(\mathbf{M}_k^{0,+}(\Gamma_1(N)) \tag{4.1}$$

grows with p as the function $\frac{r(N)}{48}p^2$. This is therefore the asymptotics with p of the number of *distinct characteristic zero* systems of Hecke eigenvalues arising from new forms of level N and weight between 2 and $p+1$.

Let now $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ be a continuous, odd, irreducible representation whose Serre's conductor is N and whose Serre's weight is k. After Serre's modularity conjecture, we know that the system of Hecke eigenvalues attached to ρ is the mod p reduction of a characteristic zero eigensystem appearing in $\mathbf{M}_{k_\rho}^0(\Gamma_1(N_\rho))$, where the integers k_ρ and N_ρ are the Serre's invariant of ρ. Moreover, it is a feature of the weight k_ρ that there exists a suitable power χ_p^h of the mod p cyclotomic character so that the Serre's weight of $\rho \otimes \chi_p^h$ is a low weight. Therefore to obtain the numerics of $R_N(p)$ that 4.1.1 predicts we had multiplied $\frac{r(N)}{48}p^2$ by p to take in account the twists of each low weight eigensystem.

The formula proposed in 4.1.1, if true, would imply that for "most" pairs of distinct characteristic zero eigensystems Φ and Φ' arising from $\mathbf{M}_k^{0,+}(\Gamma_1(N))$, where k is a low weight, we have:

i) the reduction mod p of Φ gives rise to an irreducible mod p representation ρ_Φ of conductor N, i.e. the mod p the reduction of the eigensystem stays "new";

ii) the reduction mod p of Φ and Φ' are distinct, i.e. Φ and Φ' are not congruent mod p;

iii) the mod p representation ρ_Φ is wildly ramified.

Conditions i) and ii) are implicit in the way we have proposed the numerics. Condition iii) is related to twists. More precisely, condition iii) amounts to the assumption that most mod p representations ρ as above have a unique "low weight twist".

It seems very hard to produce *lower* bounds for $R_N(p)$. Serre, in an unpublished observation (cf.[30],§8) has shown that $R_1(p) \geq cp^2$ using an estimate on Bernoulli numbers b_k that are p-regular.

4.1.3 Counting from the quaternion viewpoint

Exploiting Serre's result on the correspondence of section 3.4.5, we count what the expected number of mod p eigensystems on the algebra of mod p modular forms should be from another point of view. Here is a sketch of how it works.

By proposition 3.4.20 any mod p system of Hecke eigenvalues arising from the space of mod p modular forms of any weight k, can be realized on the space of functions

$$V^{\Psi} = \left\{ f : D^* \backslash D^*_{\mathbf{A}} / U(1,N) \to \overline{\mathbf{F}}_p \right\},$$

where Ψ is a character $\Psi : \mathbf{F}^*_{p^2} \to \mathbf{F}^*_{p^2}$ so that $\Psi(x) = x^{k'}$, for some $k' \equiv k \pmod{p-1}$. Now, if $N > 4$ the dimension of this space equals that of $V^{\mathbf{1}}$, where $\mathbf{1} : \mathbf{F}^*_{p^2} \to \mathbf{F}^*_{p^2}$ is the trivial character, as any pair (E, α) where E is a supersingular elliptic curve and α is point of order N on E, has no automorphisms.

The space $V^{\mathbf{1}}$ is the space of functions

$$V^{\mathbf{1}} : \left\{ D^*_{\mathbf{Q}} \backslash D^*_{\mathbf{A}} / U(p,N) \to \overline{\mathbf{F}}_p \right\},$$

where the open, compact subgroup $U(p,N)$ is equal to the product

$$\Pi_{\ell \neq p} U\ell(N) \times R^*_p \times D^*_{\mathbf{R}}$$

(cf. 3.4.4). By choosing now any set-theoretic lifting $\overline{\mathbf{F}}_p \subset \hat{\mathbf{Z}} \subset \mathbf{C}$, we can identify $V^{\mathbf{1}}$ with the space of function

$$\tilde{V}^{\mathbf{1}} : \left\{ D^*_{\mathbf{Q}} \backslash D^*_{\mathbf{A}} / U(p,N) \to \mathbf{C} \right\}.$$

The action of the Hecke operators T_ℓ for $\ell \neq p$ on $V^{\mathbf{1}}$ lifts the action on $V^{\mathbf{1}}$ and any mod p eigensystem occurring in $V^{\mathbf{1}}$ can be lift to an eigensystem of $\tilde{V}^{\mathbf{1}}$ (cf. [11], lemme 6.11). Let now Φ be a system of Hecke eigenvalues arising from $\tilde{V}^{\mathbf{1}}$. We have that Φ corresponds to a representation π^*_Φ of $D^*_{\mathbf{A}}$ on $L^2(D^*_{\mathbf{Q}} D^*_{\mathbf{A}}, \psi)$, for some finite order central character $\psi : \mathbf{A}^*/\mathbf{Q}^* \to \mathbf{C}^*$ of conductor supported at N. Using the Jacquet-Langlands global correspondence ([16]) we can "transfer" π^*_Φ to a cuspidal form π_Φ of $\mathrm{GL}_2(\mathbf{A})$. That is, an irreducible constituent of $L^2_0(G_{\mathbf{Q}} \backslash G_{\mathbf{A}}, \psi)$. The local component $\pi_{\Phi,\ell}$ at a prime $\ell \notin \{p, \infty\}$ of π_Φ is isomorphic to $\pi^*_{\Phi,\ell}$, $\pi_{\Phi,\infty}$ is the discrete series of lowest weight 2 and $\pi_{\Phi,p}$ is a special representation and its conductor is p. It follows from the dictionary between cuspidal forms of $G^*_{\mathbf{A}}$ and cuspidal modular forms (2.3.2) that π_Φ is identified by a unique new form f_Φ on $\mathbf{M}^{0,+}_2(\Gamma_0(N'p), \epsilon)$, where N' is the prime to p part of the conductor of π_Φ and where ϵ is a character of conductor dividing N'.

If now Φ is taken to be of exact conductor N then f_Φ is a new form of type $(2, \epsilon)$, where ϵ is a character of $(\mathbf{Z}/N)^*$. Moreover this process can be reversed, and the Jacquet-Langlands correspondence gives a bijection between cuspidal new forms on $\mathbf{M}^{0,+}_2(\Gamma_0(Np), \epsilon)$,

where the conductor of ϵ does not divide p, and systems of Hecke eigenvalues arising from the space $\tilde{V}^{\mathbf{1}}$. The dimension of $\mathbf{M}_2^{0,+}(\Gamma_1(Np))$ behaves with p, for N fixed, as $r(N)p^2/24$, (cf. [35]) and to get the asymptotics for the dimension of $\mathbf{M}_2^{0,+}(\Gamma_0(Np),\epsilon)$ we need to multiply by a factor of $1/p$ to take in account that ϵ has prime to p conductor.

In conclusion this shows that the number of characteristic zero systems of eigenvalues on $\tilde{V}^{\mathbf{1}}$ behaves like $r(N)p/24$, as p grows indefinitely. The extra factor of $p^2/2$ that we are missing in order to obtain the same asymptotics for $R_N(p)$ given in 4.1.1, comes from the fact that we need to take in account all the other isotypical components $\tilde{V}^{\Psi}$, for Ψ a nontrivial character. Keeping in mind that we have $\tilde{V}^{\Psi} \simeq \tilde{V}^{p\Psi}$, we see that we "gain" a factor that behaves as $p^2/2$.

4.2 Computations

4.2.1 Systems of eigenvalues

Let K be a perfect field and $\bar{K}$ an algebraic closure of K. Let V be a nonzero vector space over K of finite dimension d, and let $(T_n)_{n\geq 1}$ be a family of *commuting* endomorphisms of V, indexed by the positive integers. Let

$$A_K \subset \mathrm{End}_K(V)$$

be the K–subalgebra of the K–endomorphisms ring of V generated by the T_n's, it is a *finite* K–algebra. If L/K is an algebraic extension of K contained in $\bar{K}$ then V_L will denote the vector space $V \otimes_K L$, deduced from V by extension of scalars. The endomorphisms T_n's act L–linearly on V_L in a natural way, the L–subalgebra of $\mathrm{End}_L(V_L)$ that they generate is isomorphic to $A_K \otimes L = A_L$.

Assume that there exists a nonzero vector $v \in V_L$ that is a *common eigenvector* for all the T_n's, and let $\lambda_n \in L$ be the eigenvalue of T_n to which v belongs, that is $T_n(v) = \lambda_n v$.

Definition 4.2.1. The collection $\Phi = (\lambda_n)$ of eigenvalues of the T_n's relative to the common eigenvector v, is called a *system of eigenvalues* arising from the action of the T_n's on V.

We will also refer to Φ as a system of eigenvalues arising from A_K, or from V. Any system of eigenvalues $\Phi = (\lambda_n)$ defines a K–algebras homomorphism $\psi : A_K \to \bar{K}$ uniquely determined by the formula

$$\psi(T_n) = \lambda_n.$$

Conversely, we have

Lemma 4.2.2. *Let $\psi : A_K \to \bar{K}$ be any K–algebras homomorphism. Then $\Phi = (\psi(T_n))$ is a system of eigenvalues arising from V.*

Proof. We are going to show the existence of an intermediate field $K \subset L \subset \bar{K}$ and a nonzero vector $v \in V_L = V \otimes_K L$, so that

$$T(v) = \psi(T)v,$$

for all $T \in A_K$.

The ring A_K is an Artin K–algebra of finite dimension and it decomposes as a finite product

$$A_K = \prod_{1 \leq i \leq h} A_i, \tag{4.2}$$

where all the A_i's are local, Artin K–algebras. Let $e_i \in A_K$, with $1 \leq\leq h$, be the orthogonal idempotents of A_K relative to the decomposition 4.2. We have

$$1 = \sum_{1 \leq i \leq h} e_i, \quad e_i^2 = e_i, \quad e_i e_j = 0 \text{ for } i \neq j.$$

The vector space V decomposes accordingly into the direct sum

$$V = \oplus_{1 \leq i \leq h} V_i,$$

where $V_i = e_i \cdot V$. Each summand V_i is a nonzero module over A_K, the component A_j acts on V_i as zero, for $i \neq j$.

If now $\psi : A_K \to \bar{K}$ is any K–algebras homomorphism then ψ factors through a projection $A \to A_{i_0}$, for a unique $i_0 \in \{1, 2, \ldots, h\}$. The ring A_{i_0} is a local K–subalgebra of $\mathrm{End}_K(V_{i_0})$ generated by the family of commuting endomorphisms $(e_{i_0}(T_n))$ and we are reduced to proving the lemma in the special case where A_K is a local ring. Let therefore $\mathfrak{m}$ be the unique prime ideal of A_K, and let $L = A_K/\mathfrak{m}$ be the residue field, a finite extension of K. The maximal ideal $\mathfrak{m}$ consists of nilpotent elements and the homomorphism $\psi : A_K \to \bar{K}$ factors through the natural projection $A_K \to A/\mathfrak{m}$ and induces an embedding $\psi : L \to \bar{K}$, denoted by the same letter. Thank to the assumption that K is perfect, we have that L/K is a separable (finite) extension and therefore there exists a primitive element $\theta \in L$, that is $L = K(\theta)$. Let now $T_\theta \in A_K$ be any element so that $\psi(T_\theta) = \theta$, and let $f_\theta(x) \in K[x]$ be the characteristic polynomial of T_θ as K–endomorphism of V. Since T_θ satisfies $f_\theta(x)$ it follows that $\psi(T_\theta) = \theta \in L$ is an eigenvalue

of T_θ acting on V_L. Let $V(\theta) \subset V_L$ be the eigenspace of T_θ for the eigenvalue θ, we have that $V(\theta)$ is nonzero and is invariant under the action of A_K. The maximal ideal $\mathfrak{m}$ acts on $V(\theta)$ via nilpotent endomorphisms that commute with each other, thus there exists a nonzero vector $v_0 \in V(\theta)$ that is killed by $\mathfrak{m}$. Let now $T \in A_K$ be any element. Since θ is a primitive element of L/K, there exists a polynomial $g(x) \in K[x]$ and an element $m_T \in \mathfrak{m}$ so that

$$T = g(T_\theta) + m_T.$$

Observe now that $\psi(g(T_\theta)) = g(\theta)$, since $g \in K[x]$, and that the operator $g(T_\theta)$ acts as multiplication by $g(\theta)$ on v_0. It follows that

$$T(v_0) = \psi(T)v_0,$$

for all $T \in A_K$, and the proof of the lemma is complete. □

4.2.2 General set up

Let us now specialize to the case $K = \mathbf{C}$, so that V is a finite dimensional, nonzero complex vector space and $(T_n)_{n\geq 1}$ is a family of commuting endomorphisms of V. Assume furthermore that the following conditions hold

i) every endomorphism T_n is semisimple;

ii) there exists a *lattice* $\Lambda \subset V$ which is stable by the T_n's.

Recall that an endomorphism T of a vector space V over a field K is semisimple if the monic, minimal polynomial $f_T(x) \in K[x]$ of T has no repeated roots. Equivalently, T is semisimple if there exists an extension L/K so that the induced action of T on $V_L = V \otimes_K L$ can be made diagonal. In ii), by a lattice Λ we mean a finitely generated $\mathbf{Z}$–module contained in V and so that $\Lambda \otimes_{\mathbf{Z}} \mathbf{C} \simeq V$.

According to the notation established in section 4.2.1, $A_{\mathbf{C}}$ is the $\mathbf{C}$–subalgebra of $\mathrm{End}_{\mathbf{C}}(V)$ generated by all the operators T_n's. We will denote by $A_{\mathbf{Z}}$ the subring of $\mathrm{End}_{\mathbf{C}}(V)$ generated over $\mathbf{Z}$ by the T_n's.

Since all the operators T_n are semisimple and commute with each other, we have the following standard fact whose proof will be omitted:

Proposition 4.2.3. *There exists a basis of V consisting of common eigenvectors for all the endomorphisms T_n. The algebra $A_{\mathbf{C}}$ is isomorphic to $\mathbf{C}^r$, for an integer $r \geq 1$ referred to as the rank of $A_{\mathbf{C}}$.*

Let E be the set of systems of eigenvalues arising from the action of $A_{\mathbf{C}}$ on V, in the sense of definition 4.2.1. It follows from lemma 4.2.2 and proposition 4.2.3 that the cardinality $|E|$ of E is equal to the rank r of $A_{\mathbf{C}}$.

Proposition 4.2.4. *The ring $A_{\mathbf{Z}}$ is a free, finitely generated $\mathbf{Z}$–module. If $\Phi = (\lambda_n)$ is a system of eigenvalues arising from $A_{\mathbf{C}}$, then the λ_n's are algebraic integers. Furthermore, the field $\mathbf{Q}(\lambda_n)$ has finite degree over $\mathbf{Q}$.*

Proof. The existence of a lattice Λ stable by the action of all the T_n's implies that $A_{\mathbf{Z}}$ may be represented as a commutative subring of $M_d(\mathbf{Z})$, where $d = \dim_{\mathbf{C}}(V)$. The first assertion follows since $M_d(\mathbf{Z}) \simeq \mathbf{Z}^{d^2}$ as $\mathbf{Z}$–module, and any submodule of $\mathbf{Z}^{d^2}$ is finite and free. For any $n \geq 1$, the operator T_n can be represented by a matrix with integer coefficients, it follows that its (monic) characteristic polynomial has integer coefficients and the eigenvalues of T_n are algebraic integers. If $\Phi = (\lambda_n)$ is a system of eigenvalues arising from V, then the field $\mathbf{Q}(\lambda_n)$ can be generated by only finitely many λ_i's, since $A_{\mathbf{Z}}$ is of finite type over $\mathbf{Z}$, therefore $\mathbf{Q}(\lambda_n)$ has finite degree over $\mathbf{Q}$. □

We readily have the following:

Proposition 4.2.5. *Let $\Phi = (\lambda_n)$ be a system of eigenvalues for $A_{\mathbf{C}}$ and let $\sigma \in G_{\mathbf{Q}}$ be an automorphism of $\bar{\mathbf{Q}}$ over $\mathbf{Q}$. Then $\sigma \cdot \Phi = (\sigma(\lambda_n))$ is a system of eigenvalues for $A_{\mathbf{C}}$.*

Proof. Let $K \subset \bar{\mathbf{Q}}$ be a finite extension of $\mathbf{Q}$ containing λ_n, for all $n \geq 1$. Let $(\alpha_1, \ldots, \alpha_d)$ be a $\mathbf{Z}$–basis of Λ and let $v \in \Lambda \otimes_{\mathbf{Z}} K$ be a (nonzero) eigenvector belonging to Φ. If $(v_1, \ldots, v_d)$ are the coordinates of v with respect to the chosen basis of Λ, and M_n is the (integral!) matrix expressing the action of T_n with respect to the coordinate system induced by $(\alpha_1, \ldots, \alpha_d)$, then we have that $(v_1, \ldots, v_d)$ is a nonzero solution of

$$M_n(v_1, \ldots, v_d)^t = \lambda_n(v_1, \ldots, v_d)^t,$$

for all n. Applying the automorphism σ to the above matrix equations gives the existence of a nonzero, simultaneous solution of the equations

$$M_n(x_1, \ldots, x_d)^t = \sigma(\lambda_n)(x_1, \ldots, x_d)^t,$$

for all n. Therefore $\sigma \cdot \Phi$ is a system of eigenvalues for $A_{\mathbf{C}}$. □

From the proposition it follows that the Galois group $G_{\mathbf{Q}}$ acts on the set E of systems of eigenvalues of $A_{\mathbf{C}}$ arising from V. Let $\Phi^i = (\lambda_n^{(i)}) \in E$ be a system of representatives

for the space $G_{\mathbf{Q}}\backslash E$, where $1 \leq i \leq g$. Let K_i denote the number field $\mathbf{Q}(\lambda_n^{(i)})$, let O_i be the ring of integers of K_i and let f_i denote the degree $[K_i : \mathbf{Q}]$. We have that f_i is equal to the size of the $G_{\mathbf{Q}}$ orbit of Φ^i, therefore $\sum_i f_i = r$. In particular, we observe that the rank of $\prod_{1\leq i\leq g} O_i$ as $\mathbf{Z}$–module is equal to r.

Proposition 4.2.6. *The rank of $A_{\mathbf{Z}}$ as $\mathbf{Z}$–module equals r and $A_{\mathbf{Z}} \otimes_{\mathbf{Z}} \mathbf{C} \simeq A_{\mathbf{C}}$. The ring $A_{\mathbf{Z}}$ embeds as a finite index subring in the product $\prod_{1\leq i\leq g} O_i$.*

Proof. Let $r_{\mathbf{Z}}$ be the rank of $A_{\mathbf{Z}}$ as $\mathbf{Z}$–module, consider the map $\phi : A_{\mathbf{Z}} \to \prod_i O_i$ given by

$$\phi(T_n) = (\lambda_n^{(1)}, \ldots, \lambda_n^{(g)}),$$

its kernel consists of the operators of $A_{\mathbf{Z}}$ acting as zero on V and therefore ϕ is an injection of rings. As remarked before the proposition, the rank of $\prod_i O_i$ as $\mathbf{Z}$–module is r, therefore, since ϕ is injective, we must have $r_{\mathbf{Z}} \leq r$. On the other hand, by definition of $A_{\mathbf{C}}$, there is a surjective map $A_{\mathbf{Z}} \otimes_{\mathbf{Z}} \mathbf{C} \to A_{\mathbf{C}}$, from which it follows, comparing dimensions over $\mathbf{C}$, that $r \leq r_{\mathbf{Z}}$. Therefore $r = r_{\mathbf{Z}}$, $A_{\mathbf{Z}} \otimes_{\mathbf{Z}} \mathbf{C} \simeq A_{\mathbf{C}}$ and ϕ identifies $A_{\mathbf{Z}}$ with a finite index subring of $\prod_i O_i$. □

The following corollary is a strengthening of proposition 4.2.2

Corollary 4.2.7. *There is a correspondence between ring homomorphisms $\varphi : A_{\mathbf{Z}} \to \mathbf{C}$ and systems of eigenvalues Φ arising from V given by $\Phi = (\varphi(T_n))$.*

Proof. According to the proposition, the $\mathbf{C}$–algebra $A_{\mathbf{C}}$ is isomorphic to $A_{\mathbf{Z}} \otimes \mathbf{C}$. Therefore ring homomorphisms $\varphi : A_{\mathbf{Z}} \to \mathbf{C}$ correspond bijectively to $\mathbf{C}$–algebras homomorphisms $\varphi \otimes \mathbf{C} : A_{\mathbf{C}} \to \mathbf{C}$ by extension of scalars. The corollary then follows from proposition 4.2.2. □

4.2.3 Systems of eigenvalues mod p

We keep the assumptions and the notation of the previous section and we let p be any prime number. Consider the mod p reduction $\Lambda/p\Lambda = \Lambda \otimes \mathbf{F}_p$ of the lattice Λ contained in the $\mathbf{C}$–vector space V. The operators T_n's preserve Λ and act on the vector space $\Lambda \otimes \mathbf{F}_p$. The $\mathbf{F}_p$–subalgebra of $\mathrm{End}_{\mathbf{F}_p}(\Lambda \otimes \mathbf{F}_p)$ that they generate is $A_{\mathbf{Z}} \otimes \mathbf{F}_p$, the mod p reduction of the ring $A_{\mathbf{Z}}$. We can therefore speak of the systems of eigenvalues arising from the action of $A_{\mathbf{Z}} \otimes \mathbf{F}_p$ on $\Lambda \otimes \mathbf{F}_p$, in the sense of definition 4.2.1. We will refer to

them as systems of eigenvalues mod p arising from $A_{\mathbf{Z}}$, and we will denote by E_p the set that they form.

The purpose of this section is to show that any system of eigenvalues mod p arises as the mod p reduction of a system of eigenvalues of $A_{\mathbf{Z}}$, in a sense that we make precise below. It is important to observe that even though the T_n's act semisimply on $\Lambda \otimes \mathbf{Q}$ by assumption, the mod p reduction of the T_n's acting on $\Lambda \otimes \mathbf{F}_p$ need not be a semisimple operator.

As a simple example, consider the ring $A = \mathbf{Z}[x]/(x(x-p))$, which is a free $\mathbf{Z}$–module with basis $(1, \bar{x})$, where $\bar{x}$ denotes the image of $x \in \mathbf{Z}[x]$ in A. The ring A acts on itself by left multiplication and the operator given by multiplication by $\bar{x}$ describes a semisimple endomorphism of $A_{\mathbf{Q}} = A \otimes \mathbf{Q}$ whose eigenvalues are 0 and p. Multiplication by $\bar{x}$ clearly preserves the lattice A inside $A_{\mathbf{Q}}$, its reduction mod p is a nonzero operator of the space $A \otimes \mathbf{F}_p$ whose square is zero, as it can easily be checked. Therefore $\bar{x}$ acts non–semisimply on $A \otimes \mathbf{F}_p$. It can be shown that for any prime $\ell \neq p$, the operators on $A \otimes \mathbf{F}_\ell$ induced by the multiplication action of A on itself are all semisimple. This, as we shall see, is related to the fact that the ring A has exactly two distinct $\overline{\mathbf{F}}_\ell$–valued points for $\ell \neq p$, and, on the other hand, there is only one ring homomorphism $A \to \overline{\mathbf{F}}_p$, that has to send $\bar{x}$ to zero.

Proposition 4.2.8. *The set E_p of systems of eigenvalues mod p of $A_{\mathbf{Z}}$ is in bijection with the set of ring homomorphisms $\varphi : A_{\mathbf{Z}} \to \overline{\mathbf{F}}_p$. In particular, the cardinality of E_p does not exceed the rank r of $A_{\mathbf{Z}}$.*

Proof. The first part of the proposition follows from lemma 4.2.2, taking in account that any ring homomorphism $\varphi : A_{\mathbf{Z}} \to \overline{\mathbf{F}}_p$ factors through $A_{\mathbf{Z}} \to A_{\mathbf{Z}} \otimes \mathbf{F}_p$. The second part of the proposition follows from the fact that for any $\mathbf{F}_p$–algebra R of finite dimension r there are at most r distinct ring homomorphisms $\varphi : R \to \overline{\mathbf{F}}_p$. □

Let $\mathfrak{p}$ be any prime of $\bar{\mathbf{Z}}$ of residual characteristic p, fix an isomorphism $\bar{\mathbf{Z}}/\mathfrak{p} \simeq \overline{\mathbf{F}}_p$. If $\alpha \in \bar{\mathbf{Z}}$ then $\bar{\alpha} \in \overline{\mathbf{F}}_p$ denotes the reduction of α mod $\mathfrak{p}$. Let $\Phi = (\lambda_n)$ be a system of eigenvalues for $A_{\mathbf{Z}}$ and let $\psi : A_{\mathbf{Z}} \to \bar{\mathbf{Z}}$ be the associated ring homomorphism, sending T_n to λ_n. The reduction mod p of Φ is defined to be $\Phi_p = (\overline{\lambda}_n)$. We have that Φ_p is a system of eigenvalues mod p, as it follows immediately from proposition 4.2.2. Conversely

Proposition 4.2.9. *Any system Φ of eigenvalues mod p arising from $A_{\mathbf{Z}}$ is the reduction mod $\mathfrak{p}$ of a system of eigenvalues $\tilde{\Phi}$ arising from $A_{\mathbf{Z}}$. Equivalently, any ring homomorphism $\varphi : A_{\mathbf{Z}} \to \overline{\mathbf{F}}_p$ is the reduction mod $\mathfrak{p}$ of a ring homomorphism $\tilde{\varphi} : A_{\mathbf{Z}} \to \bar{\mathbf{Z}}$, for some $\tilde{\varphi}$.*

Proof. The equivalence of the two statements is a consequence of lemma 4.2.2 and corollary 4.2.7. We are going to show the validity of the second statement.

According to proposition 4.2.6, the ring $A_{\mathbf{Z}}$ is isomorphic to a finite index subring of a finite product $\prod_i O_i$, where, for $1 \leq i \leq g$, the ring O_i consists of the integers of a certain number field K_i. Let P be the maximal ideal of $A_{\mathbf{Z}}$ given by the kernel of φ. Since the extension $A_{\mathbf{Z}} \subset \prod_i O_i$ is integral, it follows from the "going up theorem" that there exists a prime ideal Q of $\prod_i O_i$, necessarily maximal, so that $Q \cap A_{\mathbf{Z}} = P$. This gives an inclusion of finite fields

$$A_{\mathbf{Z}}/P \subset \prod_i O_i/Q,$$

and the ring homomorphism $\varphi : A_{\mathbf{Z}} \to \overline{\mathbf{F}}_p$ extends to a ring homomorphism from $\prod_i O_i$ to $\overline{\mathbf{F}}_p$. This reduces the proof of the proposition to showing the validity of its second statement for the ring $\prod_i O_i$. Now since any ring homomorphism $\varphi : \prod_i O_i \to \overline{\mathbf{F}}_p$ factors through some projection $p_i : \prod_i O_i \to O_i$, we are reduced to show the statement for the ring of integers O of a number field K. This follows easily from the fact that the Galois group $G_{\mathbf{Q}}$ acts transitively on the prime ideals of $\bar{\mathbf{Z}}$ of fixed residual characteristic. □

Corollary 4.2.10. *The following are equivalent*

i) all the operators T_n's act semisimply on $\Lambda \otimes \mathbf{F}_p$;

ii) any two distinct systems of eigenvalues Φ and Φ' of $A_{\mathbf{Z}}$ are incongruent mod $\mathfrak{p}$;

iii) the cardinality of E_p equals that of E;

iv) there are exactly r distinct ring homomorphisms $\varphi : A_{\mathbf{Z}} \to \overline{\mathbf{F}}_p$.

Proof. Conditions ii), iii) and iv) are equivalent thank to proposition 4.2.9. Assume that all the T_n's act semisimply on $\Lambda \otimes \mathbf{F}_p$, then the ring $A_{\mathbf{Z}} \otimes \overline{\mathbf{F}}_p$ is isomorphic to $\overline{\mathbf{F}}_p^r$, where r is the $\mathbf{Z}$–rank of $A_{\mathbf{Z}}$, and iv) follows. Conversely iv) implies that $A_{\mathbf{Z}} \otimes \overline{\mathbf{F}}_p \simeq \overline{\mathbf{F}}_p^r$ and therefore the mod p operators T_n act semisimply on $\Lambda \otimes \mathbf{F}_p$. □

4.2.4 Discriminant

Let A be a commutative ring with identity which is a finite, free $\mathbf{Z}$–module of rank $r \geq 1$, and let $A_{\mathbf{Q}} = A \otimes \mathbf{Q}$ be the $\mathbf{Q}$–vector space deduced from A by extension of scalars. The ring A will be regarded as a subring of the endomorphisms ring $\mathrm{End}_{\mathbf{Q}}(A_{\mathbf{Q}})$ by identifying an element $a \in A$ with the $\mathbf{Q}$–linear extension of the map $l_a : A \to A$ given by left multiplication by a.

Definition 4.2.11. If $a \in A$ the *trace* $\mathrm{tr}(a)$ and the monic *characteristic polynomial* $f_a = f_a(x) \in \mathbf{Q}[x]$ of a are defined to be those of the corresponding endomorphism l_a of $A_{\mathbf{Q}}$.

If $b = (b_1, \ldots, b_r)$ is a $\mathbf{Z}$–basis of A then the map l_a is represented, in the coordinates induced by b, by a matrix M_a with integer coefficients. The trace $\mathrm{tr}(a)$ and the characteristic polynomial $f_a(x)$ of a are those of the matrix M_a. It follows that for any $a \in A$, $\mathrm{tr}(a)$ is an integer, and $f_a(x)$ has integer coefficients. Consider the ring homomorphism

$$v_a : \mathbf{Q}[x] \to \mathrm{End}_{\mathbf{Q}}(A_{\mathbf{Q}}),$$

defined by $v_a(x) = l_a$. The kernel of $v_a(x)$ is a principal ideal generated by a monic polynomial $p_a(x)$, called the *minimal* polynomial of a. We have that $p_a(x)$ divides $f_a(x)$, therefore by Gauss lemma we must have $p_a(x) \in \mathbf{Z}[x]$. Consider the bilinear form $<,>$: $A \times A \to \mathbf{Z}$ defined by

$$< x, y >= \mathrm{tr}(xy).$$

Definition 4.2.12. Let $x = (x_1, \ldots, x_r)$ be any r–uple of elements $x_i \in A$. Then the *discriminant* δ_x of x is defined to be the determinant of the $r \times r$ matrix $(\mathrm{tr}(x_i x_j))$.

In the rest of the section any r–uple $z = (z_1, \ldots, z_r)$ of elements of A will be regarded as a row vector of A^r, moreover if H is any matrix with entries in A, then $\mathrm{tr}(H)$ denotes the integer valued matrix obtained from H by applying the function tr to each of the entries of H. As usual, the symbol H^t denotes the transpose of H. Notice that, using this notation, we have $\delta_x = \det(\mathrm{tr}(x^t x))$.

Lemma 4.2.13. *Let $M \in M_r(\mathbf{Z})$ be an $r \times r$ matrix with integer entries and let $y = xM$ be the r–uple obtained from x by right multiplication by M. Then, we have $\delta_y = \det(M)^2 \delta_x$.*

Proof. By definition we have

$$\delta_y = \det(\mathrm{tr}(y^t y)) = \det(\mathrm{tr}(M^t x^t x M)).$$

Since tr is **Z**-linear and M has integer coefficients, the previous becomes

$$\det(\mathrm{tr}(M^t x^t x M)) = \det(M^t \mathrm{tr}(x^t x) M) = \det(M^t)\det(\mathrm{tr}(x^t x))\det(M) = \det(M)^2 \delta_x,$$

and the lemma is proved. □

Let now $b = (b_1, \ldots, b_r)$ be a **Z**–basis of A, then the discriminant of A is the integer defined as

$$\delta_A = \det(\mathrm{tr}(b^t b)). \tag{4.3}$$

From lemma 4.2.13 we see that δ_A is independent of the choice of the basis b. If A is the ring of integers in a number field K, then δ_A is the classical invariant δ_K of K, which is a nonzero integer.

Let A_i be a finite set of rings that are finite free as **Z**-modules, for $1 \leq i \leq n$. Their product $R = \Pi_i A_i$ is also a finite free **Z**-module and the discriminants δ_{A_i} and δ_R are defined by 4.3.

Lemma 4.2.14. *The discriminant δ_R of R is equal to the product $\Pi_i \delta_{A_i}$ of the discriminants of the A_i's. If $B \subset A$ is a subring of finite index h, then $\delta_B = h^2 \delta_A$.*

Proof. Let r_i be the rank of A_i as **Z**-module and $b^{(i)} = (b_1^{(i)}, \ldots, b_{r_i}^{(i)})$ a **Z**-basis of A_i. Then $b = (b_1^{(1)}, \ldots, b_{r_1}^{(1)}, b_1^{(2)}, \ldots, b_{r_n}^{(n)})$ is a **Z**-basis of R and the matrix $b^t b$ has n square blocks given by ${b^{(i)}}^t b^{(i)}$ along the diagonal, for $1 \leq i \leq n$, and it is zero otherwise. It follows that the determinant of $\mathrm{tr}(b^t b)$ is equal to the product of the determinants of $\mathrm{tr}({b^{(i)}}^t b^{(i)})$ and the first part of the lemma follows. The second part follows from lemma 4.2.13 and from the fact that any matrix expressing the vectors of a basis of B as a combination of vectors describing a basis of A has determinant equal to $\pm h$. □

In the special case where the ring A is *monogenic*, that is $A = \mathbf{Z}[a]$, the discriminant δ_A coincides with the discriminant of the characteristic polynomial of a. In fact let $f \in \mathbf{Z}[x]$

be a monic polynomial of degree $r \geq 1$, and let $(\alpha_1, \ldots, \alpha_r)$ be the (possibly repeated) roots of f in $\bar{\mathbf{Q}}$. The *discriminant* δ_f of f is defined as

$$\delta_{f_a} = \Pi_{1 \leq i < j \leq r}(\alpha_i - \alpha_j)^2,$$

the expression is independent of the ordering of the roots of f. The ring

$$A_f = \mathbf{Z}[x]/(f(x))$$

is a finite free $\mathbf{Z}$-module of rank r.

Lemma 4.2.15. *The discriminant δ_{A_f} of A_f equals the discriminant δ_f of the polynomial f.*

Proof. Let $\bar{x}$ be the image of $x \in \mathbf{Z}[x]$ in $A_f = \mathbf{Z}[x]/(f(x))$ and let

$$\sigma_i : A_f \to \bar{\mathbf{Q}}$$

be the ring homomorphism determined by $\sigma_i(\bar{x}) = \alpha_i$, where $(\alpha_1, \ldots, \alpha_r)$ are the roots of f. The homomorphisms σ_i's need not be pairwise distinct as f may have repeated roots. It is easy to see that for any $a \in A_f$ the trace $\mathrm{tr}(a)$ defined in 4.2.11 satisfies

$$\mathrm{tr}(a) = \sum_{1 \leq i \leq r} \sigma_i(a). \tag{4.4}$$

Let $y = (y_1, \ldots, y_r)$ be any r–uple of elements of A_f. Consider the $r \times r$ matrix H whose (i, j) entry $h_{i,j}$ is $\sigma_i(a_j)$.
Let M be the $r \times r$ matrix given by $M = H^t H$. The (i, j) entry $m_{i,j}$ of M is

$$m_{i,j} = \sum_{1 \leq k \leq r} h_{k,i} h_{k,j} = \sum_{1 \leq k \leq r} \sigma_k(y_i)\sigma_k(y_j) = \sum_{1 \leq k \leq r} \sigma_k(y_i y_j) = \mathrm{tr}(y_i y_j).$$

Therefore we have that $H^t H = \mathrm{tr}(y^t y)$, in particular $\det(H)^2 = \delta_y$.

Let now $y = (1, \bar{x}, \bar{x}^2, \ldots, \bar{x}^{r-1})$, it is a $\mathbf{Z}$-basis of A_f. Consider the $r \times r$ matrix with (i, j) term given by

$$\sigma_i(\bar{x}^{j-1}) = \alpha_i^{j-1}.$$

Thank to the previous calculation we have that $\delta_{A_f} = \det(\alpha_i^{j-1})^2$. This is a Vandermonde determinant and we have (cf. [34], 2, Th 8)

$$\det(\alpha_i^{j-1}) = \Pi_{1 \leq s < t \leq r}(\alpha_s - \alpha_t),$$

and the lemma follows. □

Let now A be any ring of the type considered in the section, and assume that $a \in A$ is an element so that the subring $\mathbf{Z}[a] \subset A$ that it generates has finite index $[A : \mathbf{Z}[a]]$. Then

Corollary 4.2.16. *We have* $\delta_{f_a} = \delta_{\mathbf{A}}[\mathbf{A} : \mathbf{Z}[a]]^2$.

Proof. This follows from lemmas 4.2.15 and 4.2.13, taking in account that if $b = (b_1, \ldots, b_r)$ is a $\mathbf{Z}$–basis of A and $b' = (b'_1, \ldots, b'_r)$ is a $\mathbf{Z}$–basis of $\mathbf{Z}[a]$, then any transition matrix M so that $b' = bM$ has determinant in absolute value equal to the index $[A : \mathbf{Z}[a]]$. □

4.2.5 A criterion for counting characteristic p points of $A_{\mathbf{Z}}$

The criterion we refer in the title of the section is based on lemma 4.2.17. Denote by ν_p the additive valuation of $\mathbf{Q}_p$, normalized so that $\nu_p(p) = 1$.

Lemma 4.2.17. *Let R be the ring of integers of a number field K of degree n, and let f denote the number of distinct characteristic p points of R. Then*

$$n - \nu_p(\delta_R) \leq f.$$

Moreover, equality holds if and only if p is tamely ramified in $\mathbf{R}$

Proof. For a prime $\mathfrak{p}$ of K above p, let $f_{\mathfrak{p}}$ and $e_{\mathfrak{p}}$ denote, respectively, the inertial degree and ramification index corresponding to $\mathfrak{p}$. There is the well–known formula (cf. [52], I §5, Prop. 10)

$$\Sigma_{\mathfrak{p}} e_{\mathfrak{p}} f_{\mathfrak{p}} = n \tag{4.5}$$

where the sum is extended to all the primes of K above p.

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

$$r_{\mathfrak{p}} \geq e_{\mathfrak{p}} - 1 \tag{4.6}$$

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

$$\nu_p(\delta_R) = \Sigma_{\mathfrak{p}} f_{\mathfrak{p}} r_{\mathfrak{p}}.$$

Taking in account formula 4.5 and the inequality 4.6, we have

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

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

Corollary 4.2.18. *If $\nu_p(\delta_{\mathbf{R}}) \leq p-1$ then p is tamely ramified in K and R has exactly $n - \nu_p(\delta_R)$ distinct characteristic p points. In particular, if $\nu_p(\delta_R) = 1$ then R has exactly $n-1$ distinct characteristic p points.*

Proof. If p is not tamely ramified in K then there exists a prime $\mathfrak{p}_0$ of K above p so that $p | e_{\mathfrak{p}_0}$ and, in the notation used in the proof of lemma 4.2.17, $r_{\mathfrak{p}_0} > e_{\mathfrak{p}_0} - 1$. In particular

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

By the proof of the lemma 4.2.17, we have

$$\nu_p(\delta_R) = \Sigma_{\mathfrak{p}} f_{\mathfrak{p}} r_{\mathfrak{p}} > p - 1$$

which completes the proof of the lemma. □

Let now $A_{\mathbf{Z}}$ be the ring introduced in section 4.2.2, and we keep the notation established there and in the following sections. In our computations we make prominent use of

Proposition 4.2.19. *Let $T_n \in A_{\mathbf{Z}}$ be any element with characteristic polynomial $f_n(x) \in \mathbf{Z}[x]$. Assume that the discriminant δ_n of $f_n(x)$ is nonzero. Then*

i) if $\nu_p(\delta_n) = 0$ then $|E_p| = |E|$;

ii) if $\nu_p(\delta_n) = 1$ then $|E_p| = |E| - 1$.

Proof. A preliminary remark is that the subring $\mathbf{Z}[T_n] \subset A_{\mathbf{Z}}$ has finite index, thank to the assumption $\delta_n \neq 0$. Equivalently, the rank of $\mathbf{Z}[T_n]$ as $\mathbf{Z}$–module is equal to that of $A_{\mathbf{Z}}$, which was denoted by r. To see this, one can observe that the $\mathbf{C}$–subalgebra of the endomorphism ring of V generated by T_n alone has rank r, since T_n has r distinct eigenvalues. Proposition 4.2.6 can be used in this setting to conclude that the ring $\mathbf{Z}[T_n]$ has rank r as $\mathbf{Z}$–module.

Consider now the formulas

$$\delta_n = [A_{\mathbf{Z}} : \mathbf{Z}[T_n]]^2 \delta_{\mathbf{A_Z}} \quad \text{(cf. prop. 4.2.16)},$$

$$\delta_{A_{\mathbf{Z}}} = [\Pi_{1 \leq i \leq g} O_i : A_{\mathbf{Z}}]^2 \Pi_{1 \leq i \leq g} \delta_{O_i} \quad \text{(cf. prop. 4.2.14, prop. 4.2.16)}.$$

In both cases i) and ii) we see that p does not divide the index $[\Pi_{1\leq i\leq g}O_i : \mathbf{Z}[T_n]]$, for otherwise we would have that $\nu_p(\delta_f) \geq 2$. It follows that the inclusions

$$\mathbf{Z}[T_n] \subset \mathbf{A} \subset \Pi_{1\leq i\leq g}O_i$$

induce the mod p isomorphisms

$$\mathbf{Z}[T_n]/p \simeq \mathbf{A}/p \simeq \Pi_{1\leq i\leq g}O_i/p,$$

and $|E_p|$ is equal to the number of characteristic p points of $\Pi_{1\leq i\leq g}O_i$, which is the sum for $i \in \{1,\ldots,g\}$ of the numbers of the characteristic p points of the O_i's. In case i) we see that p does not divide any of the δ_{O_i}'s, and therefore it is unramified in each of the O_i, which readily implies that $|E_p| = \sigma_i f_i = |E|$, where $f_i = [\mathbf{Q}(\lambda_n^{(i)}) : \mathbf{Q}]$.

In case ii) we see that p ramifies in one and only one of the rings O_i's, say O_1, we have $\nu_p(\delta_{O_1}) = 1$ and $\nu_p(\delta_{O_i}) = 0$ for $i \in \{2,\ldots,g\}$. It follows from corollary 4.2.18 that for $i \in \{2,\ldots,g\}$ the ring O_i has f_i characteristic p points and that O_1 has $f_1 - 1$ characteristic p points. Therefore the total number of characteristic p points of $\Pi_{1\leq i\leq g}O_i$ is equal to $(\sigma_i f_i) - 1 = |E| - 1$. □

4.2.6 Congruences between full level eigenforms

In this section we finally explain the method we adopt for counting how many mod p, full level eigenforms there are in weight k, where $2 \leq k \leq p+1$. It shall be point out that, however, our method does not exactly count such eigenforms but, rather, gives a way to decide if there are "many" distinct eigenforms and only "few" congruences.

Let p be a rational prime and let $2 \leq k \leq p+1$ be an even integer. Let $\mathbf{M}_k^0$ be the complex vector space of level one, cusp forms of weight k and let $\mathbf{M}_k^0(\mathbf{Z}) \subset \mathbf{M}_k^0$ be the subgroup of those form whose Fourier expansion at ∞ is with integer coefficients. We know that $\mathbf{M}_k^0(\mathbf{Z})$ is an integral structure of $\mathbf{M}_k^0$, for any k.

Let n be any integer ≥ 1, and let $T_n(k)$ be the n–th Hecke operators acting on $\mathbf{M}_k^0$. Sometimes we will write simply T_n for $T_n(k)$ if there is no risk of confusion about the weight we are working with. The family of operators $(T_n)_{n\geq 1}$ is a commuting family of semisimple operator of $\mathbf{M}_k^0$ and each T_n preserves $\mathbf{M}_k^0(\mathbf{Z})$, therefore the hypothesis of section 4.2.2 are satisfied.

Denote the finite $\mathbf{C}$–algebra generated by all the T_n's by $\mathcal{H}_k$, and the ring that they generate over $\mathbf{Z}$ by $\mathcal{H}_k(\mathbf{Z})$. The algebra $\mathcal{H}_k$ is isomorphic to $\mathbf{C}^{r_k}$, where r_k is the number of eigensystems arising from $\mathbf{M}_k^0$. By the multplicity one theorem for $\mathbf{M}_k^0$ we also have

that the rank r_k of $\mathcal{H}_k$ is equal to the dimension of the space $\mathbf{M}_k^0$ (this is because there are no old forms when the level is one). By proposition 4.2.6 the rank of $\mathcal{H}_k(\mathbf{Z})$ as $\mathbf{Z}$-module is equal to r_k.

Let E_p be the set of mod p eigensystems arising from the space $\mathbf{M}_k^0(\mathbf{Z}) \otimes \overline{\mathbf{F}}_p$.

Proposition 4.2.20. *Let n be any integer ≥ 1, consider the Hecke operator $T_n \in \mathcal{H}_k(\mathbf{Z})$ acting on $\mathbf{M}_k^0$. Let δ_n be the discriminant of the characteristic polynomial of T_n. Suppose that $\delta_n \neq 0$, then*

i) if $\nu_p(\delta_n) = 0$ then $|E_p| = r_k$;

ii) if $\nu_p(\delta_n) = 1$ then $|E_p| = r_k - 1$.

Proof. This is precisely proposition 4.2.19 applied to the given specific situation. □

What makes this criterion effective is that for a pair (p, k) as above it is typically the case that $\nu_p(\delta_2) = 0$, in the notation of the proposition (for more precise information cf. 4.2.8).

4.2.7 Companionship and supersingular systems

Before proceeding with the description of the method used for computing we present an elementar lemma. Let p be any prime number and if $f \in \mathbf{Z}[x]$ is any polynomials with integer coefficients, then $\bar{f}(x) \in \mathbf{F}_p[x]$ denotes the polynomial obtained by reducing the coefficients of $f(x)$ mod p.

Definition 4.2.21. . Let $h(x), j(x) \in \mathbf{Z}[x]$ be monic polynomials with integer coefficients and let $d_p(x) \in \mathbf{F}_p[x]$ be the greatest common divisor $(\bar{h}(x), \bar{j}(x))$ of their reductions mod p. We will say that $h(x)$ and $j(x)$ are *linked* at p if $d_p(x)$ has degree > 0. Furthermore, we will say that $h(x)$ and $j(x)$ are *one–time linked* at p if $d_p(x)$ is linear and its root $\alpha \in \mathbf{F}_p$ is a simple root for both $\bar{h}(x)$ and $\bar{j}(x)$.

Lemma 4.2.22. *Let $h(x)$ and $j(x)$ be two monic polynomials with integer coefficients, and let δ_h and δ_j denote their respective discriminants. Assume that the discriminant δ_{hj} of the product $h(x)j(x)$ is nonzero. Then*

i) $\delta_h\delta_j$ divides δ_{hj};

ii) the quotient $\delta_{hj}/(\delta_h\delta_j)$ is a square;

iii) $\nu_p(\delta_{hj}/(\delta_h\delta_j)) > 0$ if and only if $h(x)$ and $j(x)$ are linked at p;

iv) $\nu_p(\delta_{hj}/(\delta_h\delta_j)) = 2$ if and only if $h(x)$ and $j(x)$ are one–time linked at p.

Proof. Let r and s be the respective degrees of $h(x)$ and $j(x)$. Let $(\alpha_1, .., \alpha_r)$ and $(\beta_1, .., \beta_s)$ be the (possibly repeated) respective roots of $h(x)$ and of $j(x)$ in $\bar{\mathbf{Q}}$. The assumption $\delta_{hj} \neq 0$ is equivalent to the requirements that $h(x)$ and $j(x)$ both have only simple roots and that $h(x)$ and $j(x)$ are relatively prime, in particular, δ_h, $\delta_j \neq 0$. By definition we see that

$$\delta_{hj}/(\delta_h \delta_j) = \prod_{i,j} (\alpha_i - \beta_j)^2 \tag{4.7}$$

and, since the product $\prod_{i,j}(\alpha_i - \beta_k)$ is easily seen to be invariant under $G_{\mathbf{Q}}$, we conclude that $\delta_{hj}/(\delta_h \delta_j)$ is a square and i) and ii) are proved.

Let $\mathfrak{p}$ be a prime of $\bar{\mathbf{Z}}$ of residual characteristic p and fix an isomorphism $\bar{\mathbf{Z}}/\mathfrak{p} \simeq \overline{\mathbf{F}}_p$. Let $\bar{\alpha}_i, \bar{\beta}_k \in \overline{\mathbf{F}}_p$ be the reductions mod $\mathfrak{p}$ of the respective roots of $h(x)$ and $j(x)$. Consider the set

$$S = \{(i,k) | 1 \leq i \leq r, \;\; 1 \leq k \leq s\},$$

and define on S the relation C by

$$C = \left\{(i,k) | \bar{\alpha}_i = \bar{\beta}_k\right\}.$$

The set C describes the type of congruences mod $\mathfrak{p}$ between the roots of $\bar{h}(x)$ and $\bar{j}(x)$. Up to renumbering the indices, C does not depend on $\mathfrak{p}$, as it can be shown using that $G_{\mathbf{Q}}$ acts transitively on primes of $\bar{\mathbf{Z}}$ of fixed residual characteristic.
By definition, we have that $h(x)$ and $j(x)$ are linked at p if and only if the set C is not empty. Moreover, we have that $h(x)$ and $j(x)$ are one–time linked at p if and only if C has only one element.

The Galois group $G_{\mathbf{Q}}$ acts on the factors $(\alpha_i - \beta_j)$ of the product 4.7, and also acts naturally on the set S. Let I be a set of indices (i,k) representing the space $G_{\mathbf{Q}} \backslash S$, then we have that 4.7 can be written as

$$\delta_{hj}/(\delta_h \delta_j) = \prod_{(i,k) \in I} N(\alpha_i - \beta_k),$$

where if $\theta \in \bar{\mathbf{Z}}$, the norm $N(\theta)$ is defined to be the product $\prod \sigma(x)$, as σ ranges through all the embeddings of $\mathbf{Q}(\theta)$ in $\bar{\mathbf{Q}}$.

Consider the norm $N(\alpha_i - \beta_k)$, for a fixed $(i,k) \in I$, and let K be the smallest number field containing $\alpha_i - \beta_k$, with ring of integers O. Then p divides $N(\alpha_i - \beta_k)$ if and only if the ideal of O generated by the element $\alpha_i - \beta_k$ is divisible by at least one prime ideal $\mathfrak{q}$ of O whose residual characteristic is p. This means that p divides $N(\alpha_i - \beta_k)$ if and only

if there exists a prime ideal $\mathfrak{q}$ of O lying above p so that $\alpha_i \equiv \beta_k \pmod{\mathfrak{q}}$. Therefore p divides $N(\alpha_i - \beta_k)$ if and only if the $G_{\mathbf{Q}}$ orbit of (i,k) in S intersects C in at least one point, and this shows iii).

Moreover, if p exactly divides $N(\alpha_i - \beta_k)$ then the ideal $\mathfrak{q}$ of O dividing the principal ideal $(\alpha_i - \beta_k)$ is unique and has inertial degree equal to one. It is easy to see that this means that p exactly divides $N(\alpha_i - \beta_k)$ if and only if the $G_{\mathbf{Q}}$ orbit of (i,k) in S intersects C in exactly one point. From this part iv) follows readily since $\nu_p(\delta_{hj}/(\delta_h\delta_j)) = 2$ if and only if exactly one of the norms $N(\alpha_i - \beta_k)$, for $(i,k) \in I$, is divisible by p and none of them is divisible by p^2. □

Let k be an even integer in the range $(2, .., p+1)$, and let (a_ℓ), for ℓ prime $\ell \neq p$, be a system of eigenvalues mod p arising from $\mathbf{M}_k^0(\mathbf{Z}) \otimes \mathbf{F}_p$.

In order to detect the existence of a companion form for the system of mod p eigenvalues (a_ℓ), we are interested in finding a system of eigenvalues (b_ℓ), arising from $\mathbf{M}_{p+1-k}(\mathbf{Z}) \otimes \mathbf{F}_p$, so that

$$a_\ell = \ell^{k-1} b_\ell \tag{4.8}$$

for all primes $\ell \neq p$. Let then ℓ be any prime $\neq p$, and let $h_\ell(x)$ be the characteristic polynomial of the Hecke operator $T_\ell(k)$ acting on $\mathbf{M}_k^0(\mathbf{Z})$. Moreover consider the operator $\ell^{k-1}T_\ell(p+1-k)$ acting on $\mathbf{M}_{p+1-k}(\mathbf{Z})$, and let $j_\ell(x)$ be its characteristic polynomial. Lemma 4.2.22 applied to $h_\ell(x)$ and $j_\ell(x)$ gives

Proposition 4.2.23. *Let (a_ℓ) be any system of eigenvalues mod p arising from $\mathbf{M}_k^0(\mathbf{Z}) \otimes \mathbf{F}_p$. Let (b_ℓ) be system of mod p eigenvalues arising from $\mathbf{M}_{p+1-k}(\mathbf{Z}) \otimes \mathbf{F}_p$ and so that 4.8 holds. Assume that the discriminant of the polynomial $h_\ell(x)j_\ell(x)$ is nonzero. Then $h_\ell(x)$ and $j_\ell(x)$ are linked at p. Moreover, assume that (a_ℓ) is the unique system arising from $\mathbf{M}_k^0(\mathbf{Z}) \otimes \mathbf{F}_p$ for which there exists a system (b_ℓ) arising from $\mathbf{M}_{p+1-k}(\mathbf{Z}) \otimes \mathbf{F}_p$ and satisfying 4.8. Assume further that the system (b_ℓ) is the reduction mod p of a unique system of eigenvalues $(\tilde{b}_\ell)$ arising from $\mathbf{M}_{p+1-k}(\mathbf{Z})$. Then $h_\ell(x)$ and $j_\ell(x)$ are one–time linked at p.*

Similarly, the system of mod p eigenvalues (a_ℓ) is supersingular if and only if there exists a system of eigenvalues (c_ℓ) arising from $\mathbf{M}_{p+3-k}^0(\mathbf{Z}) \otimes \mathbf{F}_p$ so that

$$a_\ell = \ell^{k-2} c_\ell \tag{4.9}$$

for all primes $\ell \neq p$ (equality actually holds also at $\ell = p$). Let ℓ be any prime $\neq p$, and let $h_\ell(x)$ be, as before, the characteristic polynomial of the Hecke operator $T_\ell(k)$ acting on $\mathbf{M}_k^0(\mathbf{Z})$. Consider the operator $\ell^{k-2}T_\ell(p+3-k)$ acting on $\mathbf{M}_{p+1-k}^0(\mathbf{Z})$, and let $j_\ell(x)$ be its characteristic polynomial. Lemma 4.2.22 gives

Proposition 4.2.24. *Let (a_ℓ) be a supersingular system of eigenvalues mod p arising from $\mathbf{M}_k^0(\mathbf{Z}) \otimes \mathbf{F}_p$. Then $h_\ell(x)$ and $j_\ell(x)$ are linked at p. Assume that (a_ℓ) is the unique supersingular system arising from $\mathbf{M}_k^0(\mathbf{Z}) \otimes \mathbf{F}_p$, and, moreover, assume that the corresponding system (c_ℓ), arising from $\mathbf{M}_{p+3-k}^0(\mathbf{Z}) \otimes \mathbf{F}_p$ and satisfying 4.9 is the reduction mod p of a unique system of eigenvalues $(\tilde{c}_\ell)$ arising from $\mathbf{M}_{p+3-k}^0(\mathbf{Z})$. Then $h_\ell(x)$ and $j_\ell(x)$ are one–time linked at p.*

The two propositions will be used to rule out the existence of companion pairs of eigensystems and the existence of supersingular systems.

4.2.8 Tables

In Table 1, pairs of the form (p, k) are considered, where $p \leq 983$ is a prime number and k is an integer which is $\leq p+1$ and so that the dimension d_k of the space $\mathbf{M}_k^0(\mathrm{SL}_2(\mathbf{Z}))$ is at least two (which means that k is even and $k \geq 28$ or $k = 24$). A prime number p appearing to the left of a number k indicates that there is exactly one congruence mod p between distinct characteristic zero systems of Hecke eigenvalues arising from the space $\mathbf{M}_k^0(\mathrm{SL}_2(\mathbf{Z}))$. More precisely, for such p and k the space $\mathbf{M}_k^0(\mathrm{SL}_2(\mathbf{Z}))$ gives rise to exactly $d_k - 1$ distinct mod p systems of Hecke eigenvalues. Table 2 contains the pairs (p, k) of the same type so that the number of systems of mod p eigenvalues arising from $\mathbf{M}_k^0(\mathrm{SL}_2(\mathbf{Z}))$ is strictly less than $d_k - 1$. In the range considered there are only four such pairs. If a pair (p, k) with $p \leq 983$ and $k \leq p+1$ does not appear in neither of the Tables 1 and 2, then there are no congruences mod p between distinct eigensystems arising from $\mathbf{M}_k^0(\mathrm{SL}_2(\mathbf{Z}))$.

In Tables 3 and 4 we collect data on companion forms (f, g) in the spaces $\mathbf{M}_k^0(\mathrm{SL}_2(\mathbf{Z}))$ and $\mathbf{M}_{p+1-k}(\mathrm{SL}_2(\mathbf{Z}))$. A string $(p, k, p+1-k)$ appearing in Table 3 indicates that there exists at most one companion pair of eigensystems between the spaces indicated above. A string $(p, k, p+1-k)$ appearing in Table 4 indicates that there might be some companion pairs. Computations stop at 641. The nontriviality of the class number of $\mathbf{Q}(\sqrt{-p})$, for some $p \equiv 3 \bmod 4$ can be seen.

Tables 5 and 6 are the analog of 3 and 4 for supersingular systems. If string $(p, k, p+3-k)$ does not appear in either one of the tables, then there is no supersingular form of

Table 1. Congruence primes I

p	k	p	k	p	k	p	k
67	32	293	266	521	350	719	570
71	54	307	88	521	358	733	332
73	40	317	198	523	424	739	692
89	68	349	38	547	486	743	640
113	84	353	92	557	82	757	750
131	28	389	124	563	476	769	78
139	28	389	390	569	108	809	520
139	138	397	358	571	422	811	244
157	74	401	220	587	220	821	438
163	80	419	258	599	128	827	522
163	146	433	126	599	388	839	242
173	74	433	322	601	528	839	738
179	70	433	352	617	288	857	804
181	38	449	108	661	92	863	706
227	46	449	374	661	130	877	100
227	220	457	202	661	312	881	144
233	148	457	266	661	424	911	820
241	96	467	376	677	64	919	800
241	198	479	34	677	658	953	268
269	114	487	228	683	280	967	362
293	76	499	70	691	214	983	676
293	156	503	204	709	174	983	742

Table 2. Congruence primes II

p	k
157	70
491	246
563	282
751	376

weight k (or $p + 3 - k$) for the given prime. If the string appears in Table 5, then there is at most one supersingular form in weight k for the prime p.

TABLE 3. COMPANION PRIMES I

p	k	p+1-k	p	k	p+1-k
23	12	12	311	32	280
31	16	16	311	126	186
59	30	30	331	164	168
83	42	42	347	74	274
107	26	82	379	20	360
107	54	54	379	190	190
139	20	120	397	16	382
139	70	70	421	112	310
151	52	100	431	80	352
173	68	106	433	188	246
179	30	150	439	214	226
193	48	146	491	124	368
211	106	106	499	250	250
241	98	144	503	162	342
269	84	186	547	274	274
271	18	254	569	86	484
271	40	232	577	54	524
307	52	256	619	158	462
307	154	154	619	216	404

TABLE 4. COMPANION PRIMES *II*

p	k	p+1-k	p	k	p+1-k
47	24	24	331	166	166
71	36	36	347	174	174
79	40	40	359	180	180
103	52	52	367	184	184
127	64	64	383	192	192
131	66	66	419	210	210
151	76	76	431	216	216
167	84	84	439	220	220
179	90	90	443	222	222
191	30	162	463	232	232
191	96	96	467	234	234
199	100	100	479	240	240
223	112	112	487	244	244
227	114	114	491	246	246
229	58	172	503	252	252
239	120	120	523	262	262
251	126	126	563	282	282
263	132	132	571	286	286
271	136	136	587	294	294
283	142	142	599	300	300
311	156	156			

TABLE 5. SUPERSINGULAR SYSTEMS I

p	k	p+3-k
59	16	46
79	38	44
107	28	82
131	40	94
139	36	106
151	60	94
173	24	152
193	72	124
223	72	154
257	50	210
257	100	160
263	98	168
269	78	194
277	92	188
307	78	232
313	114	202
379	56	326
419	106	316
463	182	284
479	236	246
499	126	376
577	36	544
599	222	380
601	136	468
647	268	382

TABLE 6. SUPERSINGULAR SYSTEMS II

p	k	p+3-k
73	38	38
97	50	50
229	116	116
257	130	130
283	72	214
331	84	250
353	76	280
491	124	370

REFERENCES

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

[2] L. Atkin, J. Lehner, *Hecke Operators on $\Gamma_0(m)$*, Math. Ann. **185**, 134–160 (1970).

[3] Z. Borevic, I. Shafarevich, *Number theory*, Academic Press, New York, 1966.

[4] D. Bump, *Automorphic forms and representations*, Cambridge University Press, 1997.

[5] W. Casselman, *On Some Results of Atkin and Lehner*, Math. Ann. **201**, 301–314 (1973).

[6] T. Centeleghe, *On a result of Iwasawa on class numbers of number fields*, Available at http://www.math.utah.edu/∼centeleg/math.html

[7] K. Chandrasekharan, *Elliptic Functions*, Springer–Verlag, 1980.

[8] P. Deligne, *Formes modulaires et représentations de GL_2*, Modular Functions of One Variable II, Lecture Notes in Math. **349**, Springer–Verlag, 55–105 (1973).

[9] P. Deligne, *Formes modulaires et représentations ℓ-adiques*, Sém. Bourbaki, 1968/69, no.355.

[10] P. Deligne, M. Rapoport, *Les schémas de module de courbes elliptiques*, Modular Functions of One Variable II, Lecture Notes in Math. **349**, Springer–Verlag, 143–316 (1973).

[11] P. Deligne, J.–P. Serre, *Formes modulaires de poids* 1, Ann. Sci. Éc. Norm. Sup. **7**, 507–530 (1974)

[12] F. Diamond, J. Shurman, *A First Course in Modular Forms*, Graduate Text in Math. **228**, Springer–Verlag (2005).

[13] M. Eichler, *Quaternäre quadratische Formen und die Riemannsche Vermutung für die Knogruenzzetafunktion*, Archiv. der Math., **5**, 355–366 (1954).

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

[15] I. Gelfand, M. Graev, I. Piatetski-Shapiro, *Representation Theopry and Automorphic Functions*, Saunders Mathematics Books, 1969.

[16] S. Gelbart, *Automorphic Forms on Adele Groups*, Princeton University Press, 1975.

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

[18] B. Gross, *Heights and the Special Values of L-series*, Proceedings of the 1985 Montreal Conference, CMS Conf.Pro. **7**, 115–187 (1987).

[19] A. Ghitza, *Siegel modular forms (mod p) and algebraic modular forms*, Available at http://www.colby.edu/personal/a/aghitza/research.html

[20] R. Hartshorne, *Algebraic Geometry*, Graduate Text in Math. **52**, Springer–Verlag (1977).

[21] J. Igusa, *Class number of a definite quaternion with prime discriminant*, Proc. Nat. Acad. Sci. U.S.A. **44**, 312–314 (1958).

[22] H. Jacquet, R. Langlands, *Automorphic forms on GL*(2), Springer–Verlag, 1970.

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

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

[25] N. Katz, *P-adic properties of modular schmes and modular forms*, Modular Functions of One Variable III, Lecture Notes in Math. **350**, Springer–Verlag, 69–190 (1973).

[26] N. Katz, *A result on modular forms in characteristic p*, Modular Functions of One Variable V, Lecture Notes in Math. **601**, Springer–Verlag, 53–61 (1977).

[27] N. Katz, B. Mazur, *Arithmetic Moduli of Elliptic Curves*, Princeton University Press, 1985.

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

[29] C. Khare, *Conjectures on Finiteness of mod p Galois Representations*, J. Ramanujan Math Soc. **15**, no. 1, 23–42 (2000).

[30] C. Khare, *Modularity of Galois representations and motives with good reduction properties*, J. Ramanujan Math. Soc. **22**, no.1, 75–100 (2007).

[31] C. Khare, J.–P. Winterberger, *On Serre's conjecture for 2-dimensional mod p representations of the absolute Galois group of the rationals* Available at http://www.math.utah.edu/ shekhar/papers.html

[32] C. Khare, J.–P. Winterberger, *Serre's modularity conjecture: the odd conductor case (I)* Available at http://www.math.ucla.edu/ shekhar/papers/papers.html

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

[34] D.A. Marcus, *Number Fields*, Springer, New York, 1977.

[35] G. Martin, *Dimensions of the spaces of cusps forms and newforms on* $\Gamma_0(N)$ *and* $\Gamma_1(N)$, J. Number Theory **112**, no.2, 298–331 (2005).

[36] J. Martinet, *Character theory and Artin L-function*, Algebraic Number Fields, Edited by A. Fröhlich. Acad. Press, 1–87 (1977).

[37] H. Matsumura, *Commutative ring theory*, Cambridge University Press, 1986.

[38] K. Ribet, *Galois representations attached to eigenforms with Nebentypus* Modular Functions of One Variable V, Lecture Notes in Math. **601**, Springer–Verlag, 17–52 (1977).

[39] J. Rogawski, *Modular forms, the Ramanujan conjecture and the Jacquet-Langlands correspondence*, Available at http://www.math.ucla.edu/ jonr/eprints.html

[40] D. Rohrlich, J. Tunnel, *An elementary case of Serre's conjecture*, Pacific J. Math., Special Issue, 299–309 (1997).

[41] J.–P. Serre, *Une interprétation des congruences relatives à la fonction τ de Ramanujan* Sém. Delange-Pisot-Poitou 1967/68, no.14.

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

[43] J.–P. Serre, *Abelian ℓ-adic Representations and Elliptic Curves*, Research Notes in Mathematics **7**, A K Peters, Ltd., Wellesley, MA, 1998.

[44] J.–P. Serre, *Valeurs propres des opérateurs de Hecke modulo l*, Journées arith.Bordeaux, Astérisque **24–25**, 109–117 (1975).

[45] J.–P. Serre, *Sur les représentations modulaires de degré* 2 *de Gal*$(\bar{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54**, no.1, 179–230 (1987).

[46] J.–P. Serre, *Formes modulaires et fonctions zêta p-adiques*, Modular Functions of One Variable III, Lecture Notes in Math. **350**, Springer–Verlag, 191–268 (1973).

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

[48] J.–P. Serre, $\Delta = b^2 - 4ac$, Math. Medley, Singapore Math.Soc 13 (1985), 1–10.

[49] J.–P. Serre, *Propriétés galoisiennes des points d'order fini des courbes elliptiques*, Invent. Math. **15**, 259–331 (1972).

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

[51] J.–P. Serre, *Two letters on Quaternions and Modular Forms (mod p)*. With introduction, appendix and references by R. Livné. Israel J. Math. **95**, 281–299 (1996).

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

[53] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Pressm, 1971.

[54] J. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Text in Math. **106**, Springer–Verlag, 1986.

[55] H.P.F. Swinnerton-Dyer, *On ℓ-adic representations and congruences for coefficients of modular forms*, Modular Functions of One Variable III, Lecture Notes in Math. **350**, Springer–Verlag, 1–55 (1973).

[56] J. Tate, *Classes d'isogénie des variétés abéliennes sur un coprs fini (d'après T. Honda)*, Sém. Bourbaki 1968/69, no.352.

[57] M.-F. Vignéras, *Arithmétique des Algèbres de Quaternions*, Lecture Notex in Math. **800**, Springer–Verlag 1980.

[58] A. Weil, *Dirichlet Series and Automorphic Forms*, Lecture Notes in Math. **189**, Springer–Verlag 1971.

[59] G. Wiese, *Dihedral Galois Representations and Katz Modular Forms*, Doc. Math. **9**, 123–133 (2004).