p-adic Modular Forms

Simone Maletto

A Thesis
in
The Department
of
Mathematics and Statistics

Presented in Partial Fulfillment of the Requirements
for the Degree of Master of Science (Mathematics) at
Concordia University
Montreal, Quebec, Canada

November 2018

CONCORDIA UNIVERSITY
School of Graduate Studies

This is to certify that the thesis prepared
By: Simone Maletto.
Entitled: p-adic Modular Forms.
and submitted in partial fulfillment of the requirements for the degree of

Master of Science (Mathematics)

complies with the regulations of this University and meets the accepted standards with respect to originality and quality.
Signed by the Final Examination committee:

_____ Chair
Dr. Carlo Mazza

_____ Examiner
Prof.Dr. Bas Edixhoven

_____ Examiner
Prof.Dr. Peter Stevenhagen

_____ Supervisor
Dr. Giovanni Rosso

Approved by _____
Yogendra P. Cahubey, Cahir, Department of Mathematics

_____,2018

_____
Andé Roy, Dean, Faculty of Arts and Science

ABSTRACT

p-adic modular forms
Simone Maletto

The aim of this thesis will be introducing an analogue of the classical modular forms that can work in the p-adic environment.

To do so, we will first try to make sense of a modulo-p concept of modular forms. As the classical object is defined over the complex number there is not an immediate way to make this reduction. In order to do so, we have to utilize the q-expansion principle to obtain an "integral" object (we use the quote-on-quote to remind that the q-expansion of a modular from lives in the localization of $\mathbb{Z}$ at a prime). So the first idea will be to work with those object, to do so we will follow [8].

Once speaking of modular forms modulo p, and modulo p^n makes sense, we will start talking about the p-adic theory as described in [6]. This first construction will be quite easy, but it will have important consequences on the notion of weight of a modular form.

While the approach described above is quite natural and efficient in order to have something to work with (we will end up with q-expansion of modular forms automatically), to retrive the geometrical nature of those object will be much harder if we proceed on this path. Therefore we look at the theory of modular forms as section of the sheaf of invariant differential on the modular curve, following [3].

In the end we will end up with two different definitions, one which gives us objects that are easier to grasp (and to compute), the other which has a more clear geometric nature (which is the reason why we study modular forms in first place). The last section of this thesis show the relation between those two, proving that we can recover one object in the first form by object defined in the second way and vice-versa.

Please call me back,
I lost a flip flop

Acknowledgements

I would like to take this little space for say thank you to the people that are, in one way or another, the ones who brought me here today.

First of all I would like to thank the ALGANT graduation committee and the whole consortium, as they gave me the chance to end up "here". Those two years have been quite a ride, but I feel like I couldn't have wished for a better path.

Second off, I really must thank my advisor, Giovanni. Thank you deeply, not in my most hopeful dreams I would have thought to find such a nice person to work with.

At last comes the hardest part, here I would like to thank way too many people, so I will try to generalize the most I can, hopefully those I would like to thank will understand that those few lines are indeed for them. I would like to say thank you to my family, as a whole, even if I might make it hard to see I do love you, I really do. I would like to say thank you to my closest friends, and to those that while not being so close to me have still managed to help me in some way, or teach me something. I am quite messy, and I know I am not a paragon of niceness, but you are stuck here with me, so deal with it.

Contents

1 Background

Before we start with the p-adic theory, let us talk a little about the well known case of classical modular forms and their relation with elliptic curves.

Definition 1. let $\mathbb{H}$ be the Poincaré half-plane and let $f : \mathbb{H} \to \mathbb{C}$ be a holomorphic function on $\mathbb{H}$, then f is said to be a modular form of weight k if, for any $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ acting on $\mathbb{H}$ via $\gamma z = \frac{az+b}{cz+d}$, one has

$$f(\gamma z) = (cz + d)^k f(z) \ .$$

Moreover we require $f$to be "holomorphic at ∞", namely that it admits limit when the imaginary part diverges. A modular form is said to be a cuspidal form if the value of such limits is 0.

Is easy to see that the only odd-weighted modular form is the 0 function and, even more easily, that the space of modular forms holomorphic at ∞ of a given weight k is a complex vector space (which can be proved to be of finite dimension for any k). Such is classically denoted as $M(1, k)$. Since the limit commutes with the vector space operations the set of cuspidal modular forms is actually a subspace of $M(1, k)$, denoted with $S(1, k)$.

To have a little bit more of a grasp on those function let us recall some facts.

Fact 1. [2]

The space $M(1, k)$ is of finite dimension for any k and its dimension over $\mathbb{C}$ is

- 0 for any k odd;
- $1 + \lfloor \frac{k}{12} \rfloor$ if k is not congruent to 2 modulo 12;
- $\lfloor \frac{k}{12} \rfloor$ otherwise .

Moreover, if we call $M = \bigoplus_k M(1, k)$ the $\mathbb{C}$-algebra of modular forms of level 1 (with point-wise multiplication), and E_4, E_6 the (normalized) Eisenstein series of weight 4 and 6 respectively. One has $M \cong \mathbb{C}[E_4, E_6]$ as algebras over $\mathbb{C}$

Fact 2. The q-expansion principle:

Let f be a modular form in the variable z, via the change of variable $q = e^{2\pi i z}$ one obtain a unique expression of f as a Fourier series

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

To see this, note that by the modularity condition, applied to the matrix

$$\gamma = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

one must have

$$f(z) = 1f(z) = f(\gamma z) = f(z+1)$$

so that all modular forms are periodic and therefore admit an expression as Fourier series

One of the most important reason to study modular forms is their relation with the theory of elliptic curves.

Recall that an elliptic curve over the complex numbers can be always be seen as a quotient $\mathbb{C}/\Lambda$ where Λ is a full rank lattice in the complex plane. Given any lattice Λ one can show that such is homothetic via an element of $\mathrm{SL}_2(\mathbb{Z})$ with the action described above (note that elements of $\mathrm{SL}_2(\mathbb{Z})$ give isomorphism of lattices) to a lattice of the form $\Lambda_\tau = \mathbb{Z} \oplus \tau\mathbb{Z}$. Thus to give a lattice is equivalent to give a point in the fundamental domain of the action of $\mathrm{SL}_2(\mathbb{Z})$, so that each elliptic curve is equivalent to a point in the quotient $Y = \mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$, and its compactification (to a sphere) $X := Y \amalg \{\infty\}$ is a moduli space for the elliptic curves and is called the modular curve.

Clearly the definition of modular form seems to have some chance to translate to functions on the modular curve. The naive intuition would lead us, given a modular form f, to assign to an elliptic curve E the value $f(\tau)$ where $(1, \tau)$ is a basis of a lattice Λ_τ such that $E = E_\tau := \mathbb{C}/\Lambda_\tau$, but this approach would not work, as we can actually have a bijection (and therefore give an alternative and more geometric definition of modular form).

Definition 2. A modular form f is an assignation rule (compatible with isomorphism) that associates to a couple (E, ω) formed by an elliptic curve E and a generator of its sheaf of invariant differentials ω, a complex number $f((E, \omega))$ with the following property

- given any $\lambda \in \mathbb{C}$ $f(E, \lambda\omega) = \lambda^{-k} f((E, \omega))$
- f is holomoprhic as a function on the fundamental domain $\mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$ under the association $\tau \mapsto E_\tau \mapsto E$.

Clearly, given a modular form in the meaning of Definition 1, one can easily find a modular form in the sense of Definition 2 setting $f((E_\tau, dz)) = f(\tau)$ for dz being the push forward of the canonical differential on $\mathbb{C}$. Conversely given any modular form f of weight k as in Definition 2, one can immediately define a function from the fundamental domain to $\mathbb{C}$ setting $f(\tau) = f(E_\tau, dz)$. For any $\tau' \in \mathbb{C}$ if τ' doesn't belong to our fundamental domain it must exists a $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$ and a τ in the fundamental domain such that $\tau' = \gamma\tau$, and hence $E_\tau = E'_\tau$ so we can extend our definition above setting $f(\tau') = f(\tau', dz')$, the question is whether or not such is a modular form. Now notice that, as $E_\tau = E'_\tau$

$$f(\tau') = f((E_{\tau'}, dz')) = F(E_{\tau'}, (c\tau+d)^{-1}dz) = (c\tau+d)^{-(-k)} f((E_\tau, dz)) = (c\tau+d)^k f(\tau)$$

which shows modularity and thus the equivalence of the definitions.

The goal of this work will be define in two different ways p-adic modular form using the approaches of Serre (which focuses on the q-expansion principle) and Katz (which bases is definition on the more geometric Definition 2) respectively and show that again we end up with the same mathematical object.

One can actually parametrize elliptic curves with extra structure, called enhanced elliptic curves or elliptic curves with a level-n structure. To do so one consider a particular subgroup $\Gamma(n)$ of $\mathrm{SL}_2(\mathbb{Z})$, called the principal congruence subgroup of level n, defined as the kernel of the projection
$\pi : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$. The quotient $\mathbb{H}/\Gamma(n)$ is a moduli space that parametrizes triplets (E, P, Q), where E is an elliptic curve and $P, Q \in {}_nE$ which generates ${}_nE$ such that the Weil pairing $e_n(P, Q) = e^{\frac{2\pi i}{n}}$.

Naturally one can talk about modular forms for those subgroups, just by restricting the definition to the elements of $\Gamma(n)$, to get results about the dimension about this vector space is now more complicated, as we need to introduce the concept of cusps.

Definition 3. Let $\Gamma(n)$ be the principal congruence subgroup of level n for $SL_2(Z)$, a cusp for $\Gamma(n)$ is an equivalence class of elements of $\mathbb{P}^1(\mathbb{Q})$ for the action of Γ given by the rule

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} (m : n) = (am + b : cn + d)$$

This concept (that might puzzle at first glance) is just the generalization of the role that has the infinity in the case of $\mathrm{SL}_2(\mathbb{Z})$ in compactifying the modular curve. If we now denote $\mathrm{SL}_2(\mathbb{Z})_\infty$ as the stabilizer of infinity under the action, and for any cusp $[t]$ we choose a representative t and call γ_t an element of $\mathrm{SL}_2(\mathbb{Z})$ that realizes $\gamma_t\infty = t$. Then we can describe the stabilizer of the cusp in $\Gamma(n)$ as $\Gamma_t(n) = \Gamma(n) \cap \gamma_t \mathrm{SL}_2(\mathbb{Z})_\infty \gamma_t^{-1}$. Moreover we get immediately an isomorphism with the subgroup $H_{[t]} = \gamma_t^{-1}\Gamma(n)\gamma_t \cap \mathrm{SL}_2(\mathbb{Z})_\infty$ of $\mathrm{SL}_2(\mathbb{Z})$. In order to find out the dimension of our spaces of modular forms one needs to associate to each cusp c a number $h(c)$, called the height of the cusp.

Fact 3. [2, Section 3.2]

Let H be a subgroup of $\mathrm{SL}_2(\mathbb{Z})_\infty$ of finite index, then H is one of the following

- $\left\langle \begin{bmatrix} 1 & h \\ 0 & 1 \end{bmatrix} \right\rangle$
- $\left\langle \begin{bmatrix} -1 & h \\ 0 & -1 \end{bmatrix} \right\rangle$
- $\left\langle \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 1 & h \\ 0 & 1 \end{bmatrix} \right\rangle$

Definition 4. Let c be a cusp, H_c the stabilizer of c in $\Gamma(n)$ seen as a subgroup of $\mathrm{SL}_2(\mathbb{Z})_\infty$ then, the height h_c of c is the h obtained in the fact above.

If our modular curve admits at least one regular cusp (we won't define what being regular actually means, as it would take more time than needed, but such condition holds whenever $\begin{bmatrix} 1 & h \\ 0 & 1 \end{bmatrix}$ belongs to H_c.) we can find an upper bound on the space of modular forms in the form of the following

Fact 4. If $\Gamma(n)$ has at least one regular cusp, $k \in \mathbb{Z}_{\geq 0}$, let $\bar{\Gamma(n)}$ be the image of $\Gamma(n)$ under the projectivization map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{PSL}_2(\mathbb{Z})$, Then one has $\dim(M_k(\Gamma(n))) = 1 + \left\lfloor \frac{k}{24}[\mathrm{PSL}_2(\mathbb{Z}) : \bar{\Gamma}(n)] \right\rfloor$.

One can actually find more precise formulas in [2]

As one can imagine, reducing our subgroup (and trying to parametrize objects with more structure) will give us "bigger" curves, in particular the compactification of the quotient $\mathbb{H}/\Gamma(n)$ (i.e. the object we get when we add the cusps) will still be a Riemann surface of (potentially) larger genus, which will be given, for $N = p \geq 5$ a prime, by the formula:

$$g = \frac{1}{24}(p+2)(p-3)(p-5) \ .$$

1.1 Elliptic curves over finite fields

We want to recall few properties about elliptic curves, especially in the case of elliptic curves over a finite field $\mathbb{F}_{p^n}$. First of all we quote the following classical result (on which we will base the definition of elliptic curve at the beginning of Section 3).

Fact 5. [7, Proposition 3.4]

Let E be an elliptic curve then the map $E \to \mathrm{Pic}^0(E)$ defined by $P \mapsto [P]-[0]$ allows us to recover the group structure of E by looking at its Picard group (this "justifies") the definition of elliptic curve over a scheme that we will give in section 4.

In the category of elliptic curves the morphism are given by isogenies which are morphisms (as algebraic varieties) that respect the group structure.

Fact 6. [7, pp 70]

Let $\phi : E_1 \to E_2$ be an isogeny between two elliptic curves, then $\mathrm{Im}(\phi) = 0$ or ϕ is surjective

Note that we have, given any non-trivial isogeny ϕ, an injective map of fields

$$\phi^\star : \bar{K}(E_2) \to \bar{K}(E_1)$$

form this one can define the degree of the isogeny $\deg(\phi)$ and the separable and inseparable degree, denoted by $\deg_s(\phi)$ and $\deg_i(\phi)$ respectively by the corresponding notion for the associated extension of fields $\bar{K}(E_1)/\phi^\star(\bar{K}(E_2))$. We set $\deg[0] = 0$ by convention.

As elliptic curves are algebraic groups we have that the set $\mathrm{End}(E)$ of endomorphisms of E is a group, moreover we can endow it with a ring structure

by using composition as multiplication law. With this structure $\mathrm{End}(E)$ can be proven to be of characteristic 0 (note that most of the times, if E is defined over a ring of characteristic 0, $\mathrm{End}(E) \cong \mathbb{Z}$ and we say that an elliptic curve has complex multiplication when the endomorphism ring is larger than $\mathbb{Z}$).

Definition 5. Given an isogeny $\phi : E_1 \to E_2$ we have an induced map at the level of Pic^0, namely $\phi^\star : \mathrm{Pic}^0(E_2) \to \mathrm{Pic}^0(E_1)$, and from what we have said in Fact 5 we can define the dual isogeny $\check{\phi}$ via the composition

$$E_2 \to \mathrm{Pic}^0(E_2) \xrightarrow{\phi^\star} \mathrm{Pic}^0(E_1) \to E_1 \ .$$

Let us now move to the case of finite characteristic.

Definition 6. Let E be an elliptic curve over $\mathbb{F}_{p^n}$ (or any perfect field of positive characteristic) and let ϕ_r be the isogeny induced on E by the r-th power of the Frobenius endomorphism. Then E is said to be supersingular if one of the following equivalent conditions holds:

- ${}_{p^r}E = 0$ for all $r \geq 1$;
- $\check{\phi}_r$ is (purely) inseparable for $r = 1$ (which implies its inseparable for all $r \geq 1$);
- $[p] : E \to E$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$;
- the formal group $\hat{E}$ of E has height 2.

If those do not hold we have ${}_{p^r}E \cong \mathbb{Z}/p^r\mathbb{Z}$ for all $r \geq 1$ and $\hat{E}$ has height 1, in such case we will say that E is ordinary.

Proof. We only prove the equivalence between the first two conditions.

Let K be a field of positive characteristic p, $r \geq 1$ and call $\phi_r : E \to E^{(p^r)}$ the r-th power of Frobenius and $\check{\phi}_r : E^{p^r} \to E$ the dual isogeny, we want to show that ${}_{p^r}E = \{0\}$ if and only if $\check{\phi}_r$ is purely inseparable.

As the Frobenius map ϕ is purely inseparable and $[p] = \check{\phi} \circ \phi$, one has

$$\deg_s(\check{\phi}_r) = \deg_s([p^r]) = (\deg_s([p]))^r = (\deg_s(\check{\phi}))^r$$

As $\#\phi^{-1}(0) = \deg_s(\phi)$ we have $\#_{p^r}E = \deg_s(\check{\phi}_r) = (\deg_s(\check{\phi}))^r$ and we are done $\square$

To conclude this part let us introduce the concept of Hasse invariant of an elliptic curve and prove that the supersingular elliptic curves are exactly those for which such vanishes. Let $p > 2$, then we have the following

Theorem 1. *Let K be a finite field of characteristic p and let E be an elliptic curve defined over K with Weierstrass equation $y^2 = f(x)$, where $f(x) \in K[x]$ is a cubic polynomial with distinct roots in $\bar{K}$. Then E is supersingular if and only if the coefficient of x^{p-1} in $(f(x))^{\frac{p-1}{2}}$ (namely, the Hasse invariant) is* 0

Proof. Let $q = \#K$, and let $\chi : K^\star \to \{\pm 1\}$ be the unique non-trivial character of order 2 (namely, the Legendre symbol) and extend it to K by setting $\chi(0) = 0$, then χ can be used to count the K-rational points of E by the formula

$$\#E(K) = 1 + q + \sum_{x \in K} \chi(f(x))$$

Since $K^\star$ is of order $q-1$, for any $z \in K$ we have $\chi(zeta) = z^{\frac{q-1}{2}}$, hence

$$\#E(K) = 1 + q + \sum_{x \in K} f(x)^{\frac{q-1}{2}} \ .$$

As $K^\star$ is cyclic we have

$$\sum_{x \in K} x^i = \begin{cases} 0 & \text{if } q-1 \nmid i \\ -1 & \text{if } q-1 \mid i \end{cases} \ .$$

Since $f(x)$ has degree 3 the only non-zero term of the sum must come form the $q-1$ degree term of $f(x)^{\frac{q-1}{2}}$. Call A_q the coefficient of x^{q-1} in $f(x)^{\frac{q-1}{2}}$ then

$$\#E(K) = 1 + A_q \ .$$

(Note that this equality holds in K and therefore is, in some sense, an equality modulo p).

On the other hand call ϕ the q-th power Forbenius endomorphism, we have

$$\#E(K) = \deg(1 - \phi) = 1 - a + q$$

(deine $a := 1+q-\deg(1-phi)$ and we have $[a] = \phi + \hat{\phi}$) so that clearly $A_q = -a$ in K. Since a is an integer we have now shown that $A_q = 0$ if and only if $a \equiv_p 0$. But $\hat{\phi} = [a] - \phi$ so we have that $a \equiv_p 0$ is equivalent to $\hat{\phi}$ being inseparable and hence E being supersingular.

This proves that $A_q = 0$ if and only if E is supersingualr, we have now to prove that $A_q = 0$ if and only if $A_p = 0$, to do so we write

$$f(x)^{\frac{p^{r+1}-1}{2}} = f(x)^{\frac{p^r-1}{2}} (f(x)^{\frac{p-1}{2}})^{p^r}$$

and equate the coefficients (recall that $f(x)$ has degree 3), obtaining

$$A_{p^{r+1}} = A_{p^r} + A_r^{p^r}$$

which gives us the result by inducing over r.

□

One can actually prove that the number of supersingular elliptic curves over a field of characteristic $p \geq 3$ is finite and is given by the number

$$\lfloor \frac{p}{12} \rfloor + \varepsilon_p$$

where $\varepsilon_3 = 1$ and for $p \geq= 5$, $\varepsilon_p = 0, 1, 1, 2$ for p respectively congruent to $1, 5, 7, 11$ modulo 12.

1.2 The Tate curve

In the first section of this introduction we heavily used the identification between an elliptic curve E over $\mathbb{C}$ and a quotient of $\mathbb{C}$ by a lattice Λ. In the case of local fields there is no reason to suppose we would be able to do the same, as it might quite probably be that a local field K has no discrete additive subgroups. Luckily we can solve this problem by noting that the exponential map $z \mapsto q = e^{2\pi i z}$ on $\mathbb{C}$ sends a lattice to a subgroup of $\mathbb{C}^\star$ and this seems way more promising, as the multiplicative group of a local field $K^\star$ has actually a lot of discrete subgroups (namely, those of the form $q^{\mathbb{Z}}$ where q is any element with valuation different form 1). For example the protagonist of this subsection is the curve over $\mathbb{Z}[[q]]$, called the Tate curve given by

$$\text{Tate}(q) : y^2 + xy = x^3 + a_4 x + a_6 \ ,$$

where the coefficients are

$$a_4 = -5 \sum_{n \geq 1} n^3 \frac{q^n}{1-q^n} \ ; \ a_6 = \frac{-1}{12} \sum_{n \geq 1} (7n^5 + 5n^3) \frac{q^n}{1-q^n} \ .$$

Note that, over the power series ring $\mathbb{Z}[[q,u]]$ this curve has the point (x,y) given by the formulas

$$x = x(q,u) = \sum_{n \in \mathbb{Z}} \frac{q^n u}{(1-q^n u)^2} - 2 \sum_{n \geq 1} \frac{nq^n}{1-q^n}$$

$$y = y(q,u) = \sum_{n \in \mathbb{Z}} \frac{q^{2n} u^2}{(1-q^n u)^3} + \sum_{n \geq 1} \frac{nq^n}{1-q^n} \ .$$

Now we can note that this makes sense if q and u are elements of the multiplicative group $K^\star$, provided that the valuation of q is less then 1. In other words, those power series will, under this condition, always converge in the natural metric, hence we get an uniformization:

$$\phi : K^\star / q^{\mathbb{Z}} \to \text{Tate}(q)(K)$$

$$u \mapsto (x(q,u), y(q,u)) \ .$$

More generally the power series above will converge for any $u \in \bar{K}$ so that we have an induced map

$$\phi : \bar{K}^\star / q^{\mathbb{Z}} \to \text{Tate}(q)(\bar{K}) \ .$$

(Note that such algebraic closure is not complete, but it suffices to work to the finite extension $K(u)$, or alternatively with the completion of the algebraic closure, which will turn out to be still algebraically closed). As the action of the absolute Galois group G_K is continuous ϕ is an isomorphism of G_K-modules, so it can lead to arithmetic deductions.

We have the following result, due to Tate (although he never published it).

Theorem 2. *(Tate)*
Let K be a field, complete with respect to a discrete valuation v.

- *for every $q \in K^\star$, such that $|q|_v < 1$, the map*

$$\phi : \bar{K}^\star / q^{\mathbb{Z}} \to \mathit{Tate}(q)(\bar{K})$$

described above is an isomorphism of G_K modules.

- *For every $j_0 \in K^\star$, with $|j_0|_v < 1$, there is a $q \in K^\star$ such that the elliptic curve $\mathit{Tate}(q)/K$ has j-invariant j_0. $\mathit{Tate}(q)$ is characterized by $j(\mathit{Tate}(q)) = j_0$ and the fact that has split multiplicative reduction at v (Note that $j(\mathit{Tate}(q)) = \frac{1}{q} + \dots$ and we can take $q = q(j)$ its inverse function).*

- *Let R be the ring of integers of K. Then under the isomorphism $\mathit{Tate}(q)(K) \cong K^\star/q^{\mathbb{Z}}$ we have identifications*

$$(\mathit{Tate}(q))_0(K) \cong R^\star \text{ and } (\mathit{Tate}(q))_1 \cong \{u \in R^\star : u \cong 1 \bmod v\} \ .$$

Where we denote with E_t the specialization of an elliptic curve $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ at t, meaning the elliptic curve given by the equation obtained by evaluating the coefficients a_i at t.

- *Let E/K be an elliptic curve with non-integral j-invariant which does not have split multiplicative reduction. Then there is a $q \in K^\star$ such that $j(E) = j(\mathit{Tate}(q))$, and therefore a unique quadratic extension L/K such that $E \cong \mathit{Tate}(q)$ over L.*

In section 3 we will use the existence of the Tate curve (and of the canonical differential on it given by $\frac{dq}{q}$) to recover a notion of q-expansion for modular forms when defined following Katz's approach.

2 Modular Forms modulo p and p-adic modular forms à la Serre

Before we start with the mathematics, let us introduce a bit of context to the theory, at least in the form of a motivation for our study, we start with recalling a (potentially) unexpected result, due Ramanujan, on the coefficients of modular forms. Let Δ be the discriminant modular form of weight 12 for $\mathrm{SL}_2(\mathbb{Z})$, and denote G_k the Eisenstein series of weight k, then we know that $G_k = \frac{\zeta(1-k)}{2} + \sum_{n=1}^{\infty} \sigma_{k-1}(n)q^n$. Analogously define $\tau(n)$ by $\Delta(q) = \sum_{n=1}^{\infty} \tau(n)q^n$, then we have

$$G_{12}(q) = \frac{691}{65520} + q + \dots$$
$$\Delta(q) = 0 + q + \dots$$

Therefore, the q-expansion of the difference (seen with coefficients in $\mathbb{Z}_{(691)}$) is given by $\frac{691}{65520} + 0q + \dots$. When we reduce modulo 691, such q-expansion becomes $0 + 0q + \dots$, and since we started with a 2-dimensional vector space we have that the only modular form of level 1 and weight 12 whose q-expansion starts with two 0 coefficients is the trivial form. Hence it must be $\sigma_{11}(n) \equiv_{691} \tau(n)$, and up to the localization above $\Delta \equiv_{691} G_{12}$. This result seems quite surprising considering what we know about modular forms, so we try to ask ourself what does it mean for two modular forms over $\mathbb{Z}$, $f \in M_k$, $g \in M_{k'}$ to be congruent modulo a prime number p.

Let now f, g be two Eisenstein series over $\mathbb{Z}$ of weight k and k' respectively, if we suppose that $f \equiv_p g$ then, as f, g are modular, it must be $d^{k-1} \equiv_p d^{k'-1}$ for all d. This means that $d^{k-k'} \equiv_p 1$ which means that $k - k'$ annihilates $\mathbb{F}_p^\star$, i.e. $p - 1 | k - k'$. Moreover, we have the following interesting result due to Kummer[4, pp 48-49]: $\frac{p}{2}\zeta(2-p)$ is congruent to 1 modulo p. If we normalize properly our Eisenstein series, calling $E_k = \frac{2}{\zeta(1-k)} G_k$ we have

$$E_{p-1} = \frac{2}{\zeta(2-p)} G_{p-1} = 1 + \sum_{n=1}^{\infty} \frac{2}{\zeta(2-p)} \sigma^{p-1}(n) q^n \equiv 1 \bmod p \ .$$

Before we go further with the modulo p theory, let us recall some result and introduce notation. From now on we will write (following Ramanujan) $R := E_6, Q := E_4$ and $P := E_2$, note that P is not a modular form on its own but satisfies very similar functional equations. Now we recall that we have a differantial $\theta := q\frac{d}{dq}$ on the space of modular form and that, if $f \in M_k$ we have $(12\theta f - kPf) \in M_{k+2}$. This follows by the identities:

$$3\theta Q - PQ = -R, \ 2\theta R - PR = -Q^2;$$
$$12\theta P - P^2 = -Q, \ \theta\Delta - P\Delta = 0.$$

So that, in the terms of the operator $\partial := 12\theta - kP$ acting on modular forms of weight k, what we have just said can be rewritten as:

Fact 7. ∂ is a derivation on the graded algebra of modular forms such that $\partial Q = -4R$ and $\partial R = -6Q^2$

We know that the space M of the modular forms is obtained as the direct sum of the spaces M_k of modular forms of weight k, and that the element of those are of the form $\sum a_n q^n$, so that we can define $\tilde{M_k} \subset \mathbb{F}_p[[q]]$ as the space obtained by the reduction modulo p of the coefficients, and hence we can consider $\tilde{M}$, the $\mathbb{F}_p-$algebra of modular forms modulo p, to be the direct sum of those spaces. Now we would like to have a more explicit description of this space.

Recall that $M \equiv \mathbb{Z}[Q, R]$, so that any element of M can be written as a polynomial $\phi(Q, R)$ and any modular form $f \in M_k$ admits a unique writing as an isobaric polynomial $\phi_f(Q, R)$. Thus each element of M can be seen as a unique finite sum of isobaric polynomials $\phi_{k_1}(Q, R) + \cdots + \phi_{k_n}(Q, R)$. Moreover this identifications clearly extends to $\mathbb{F}_p$, so that we can express the image of M_k as the set $\{\tilde{\phi}_f(\tilde{Q}, \tilde{R}) | f \in M_k\}$ (where the tilde represents the reduction modulo p).

Hence, in the end we want to study the ring homomorphism

$$M \xrightarrow{\psi} \mathbb{F}_p[[q]]$$

as its image is our space $\tilde{M}$ of modular forms modulo p. Now define $A := E_{p-1}$ and $B := E_{p+1}$, then we have the following

Theorem 3. *[8]*
Let $p \geq 5$, then

1. $\tilde{A}(\tilde{Q}, \tilde{R}) = 1$ *and* $\tilde{B}(\tilde{Q}, \tilde{R}) = \tilde{P}$;
2. $\partial\tilde{A}(\tilde{Q}, \tilde{R}) = \tilde{B}(\tilde{Q}, \tilde{R})$ *and* $\partial\tilde{B}(\tilde{Q}, \tilde{R}) = -Q\tilde{A}(\tilde{Q}, \tilde{R})$;
3. $\tilde{A}(\tilde{Q}, \tilde{R})$ *has no repeated factor and is prime to* $\tilde{B}(\tilde{Q}, \tilde{R})$;
4. $\mathrm{CoKer}(\psi) = \mathbb{F}_p[\tilde{Q}, \tilde{R}]/(\tilde{A}(\tilde{Q}, \tilde{R}) - 1)$

Proof. 1. We already explained $\tilde{A}(\tilde{Q}, \tilde{R}) \equiv 1$. Since $d \equiv_p d^p$, we have $\sigma_1(n) \equiv \sigma_p(n)$ for all n, and hence $\tilde{P} \equiv_p \tilde{B}(\tilde{Q}, \tilde{R})$.

2. Since $\tilde{A}(\tilde{Q}, \tilde{R}) \equiv 1$, $\theta\tilde{A}(\tilde{Q}, \tilde{R}) = 0$, so that we have

$$\partial\tilde{A}(\tilde{Q}, \tilde{R}) = \tilde{P}\tilde{A}(\tilde{Q}, \tilde{R}) = \tilde{P} = \tilde{B}(\tilde{Q}, \tilde{R}) \ .$$

and also

$$\partial\tilde{B}(\tilde{Q}, \tilde{R}) = (12\theta - \tilde{P})\tilde{B}(\tilde{Q}, \tilde{R}) = (12\theta - \tilde{P})\tilde{P} = -\tilde{Q}.$$

A similar argument shows that $\partial\tilde{B}(Q, R) = -Q\tilde{A}(Q, R)$.

3. Suppose now that it exists an $n \geq 1$ such that $(Q^3 - cR^2)^n$ divides exactly $\tilde{A}$ for some c algebraic over $\mathbb{F}_p$. Since $\tilde{A}(0,0) \neq 0$ and $(Q^3 - R^2)(0,0) = 0$ c must be different form 1, so that we have

$$\partial(Q^3 - cR^2) = 12(c-1)Q^2R \ .$$

Which is prime to $Q^3 - cR^2$. Now, since we proved $\partial\tilde{A} = \tilde{B}$, we have that $(Q^3 - cR^2)^{n-1}$ divides exactly $\tilde{B}$ and therefore, if $n \geq 2$ we have that $(Q^3 - cR^2)^{n-2}$ divides exactly $\tilde{A}$, which is absurd. A similar argument works for powers of Q and R, hence $\tilde{A}$ has no repeated factors, and its simple factors do not divide $\tilde{B}$

4. Let $\mathfrak{a} = \mathrm{Ker}(\mathbb{F}_p[Q,R] \to \mathbb{F}_p[[q]])$ obtained by substitution, we proved that $(\tilde{A}(Q,R) - 1) \in \mathfrak{a}$. As the codomain is an integral domain, $\mathfrak{a}$ must be a prime ideal, containing $\tilde{A}(Q,R) - 1$, now we see that $\mathfrak{a}$ cannot be maximal, as this would imply that Q, R are algebraic over $\mathbb{F}_p$. So that $\mathfrak{a}$ has height 1, and if we prove that $\tilde{A} - 1$ is prime we are done. Seeking for a contradiction, we assume the thesis to be false, and write $\phi(Q,R)$ for an irreducible proper factor of $\tilde{A} - 1$, let $\phi(Q,R) = \phi_n(Q,R) + \phi_{n-1}(Q,R) + \cdots + 1$ be the decomposition of $\phi(Q,R)$ in isobaric polynomials, were the subindex indicates the respective weight, and let $\nu \in \mu_{p-1}(\mathbb{F}_p)$ primitive. Then $\tilde{A}(\nu^2 Q, \nu^3 R) = \tilde{A}(Q,R)$ and hence $\phi(\nu^2 Q, \nu^3 R)$ is also a factor of $\tilde{A}(Q,R) - 1$, and it is different form $\phi(Q,R)$ and hence prime to it, so that the product of the two must divide $\tilde{A}(Q,R) - 1$. Now, $\phi_n(Q,R)\phi_n(\nu^2 Q, \nu^3 R) = \phi_n(Q,R)^2$ and must divide $\tilde{A}(Q,R)$ as those are the isobaric component of maximum degree in the expressions, but this is absurd by what we have just proved.

□

2.1 Modular forms (for level 1) à la Serre

Following [6] ,now that we have made some sense of what is a modular form modulo p, we want to define $p-$adic modular forms, as the whole purpose of this thesis will be understanding what those are. To do so we can follow two main approaches, based on two big concepts related to modular forms: the q-expansion principle and the relation between modular forms and elliptic curves. In order to provide a more linear argument, we start with Serre's take on the question, based on the q-expansion principle.

We define a valuation on $\mathbb{Z}[[q]]$ by setting $v_p(f) = \inf_n v_p(a_n)$. This valuation defines a norm on $\mathbb{Z}[[q]]$ in the usual way, and we define a p-adic (integral) modular form to be an element of the completion of $\mathbb{Z}[[q]]$ (or even $\mathbb{Z}_p[[q]]$) with respect to this $p-$norm. Now we want to show that we can recover a notion of "weight" for those object, but before we do so let us point out something more about the structure of the $\mathbb{F}_p$-algebra $\tilde{M}$ of modular forms modulo p.

By Theorem 1 we have that the map given by multiplication by $\tilde{A}(Q,R)$ on $\mathbb{F}_p[Q,R]$ induces the identity map on $\tilde{M}$, so that we can decompose this algebra

as the union of $p-1$ components $\tilde{M}^\alpha := \bigcup_{k\equiv_{p-1}\alpha} \tilde{M}_k$ so that $\tilde{M} \cong \bigoplus_{[\alpha]\in\mathbb{Z}/(p-1)\mathbb{Z}} \tilde{M}^\alpha$ where α varies in a family of representatives for $\mathbb{Z}/(p-1)\mathbb{Z}$. One can actually prove that $\tilde{M}^0$ and M are both Dedekind domains, fact that we will (partially) use in the proof of the following

Theorem 4. *Let $p \geq 3$ and $m \geq 1$ be an integer, and let f, f' be modular forms for $\mathrm{SL}_2(\mathbb{Z})$ over $\mathbb{Q}$ of weights k and k' respectively and assume $f \neq 0$ and $v_p(f - f') \geq v_p(f) + m$.*

Then we have $k' \equiv k$ modulo $(p-1)p^{m-1}$

Proof. Note that, up to scalar multiplication, we can assume $v_p(f) = 0$ and hence we can rewrite the hypothesis as $f \equiv f' \bmod p^m$ so that, if the coefficients of f and f' are $p-$integers, we have $\tilde{f} = \tilde{f}' \neq 0$ and, if $p \geq 5$ f and f' belongs to the same $\tilde{M}^\alpha$ and $k \equiv k' \bmod p-1$. Now we have to prove the case $p = 3$. Assume $m \geq 2$ and set $h = k' - k$, up to replacing f' with $f' E_{p^n(p-1)}$ for n big enough we can assume $h \geq 4$, so that the Eisenstein series E_h is a modular for of weight h, and as $p-1$ divides h one has $E_h \equiv_p 1$. Now fix $r := v_p(h) + 1$, we claim that $r \geq m$. Once more, we assume the thesis to be false, so that $m < r$, then we have $fE_h - f' = f - f' + f(E_h - 1)$, but we know that $f \equiv_{p^m} f'$ and $E_h - 1 \equiv_{p^r} 0$ so that $fE_h - f' \equiv_{p^r} 0$ and hence

$$p^{-r}(fE_h - f') \equiv_p p^{-r} f(E_h - 1) \ .$$

By Clausen-Von Staudt, we can decompose $p^{-r}(fE_h - f') = \lambda\phi$ where $\phi = \sum_{n=1}^{\infty} \sigma_h(n) q^n$ and λ is prime to p, so that the congruence above gives us

$$f\phi \equiv_p g$$

where g is the modular form $(\lambda p^r)^{-1}(fE_h - f')$ of weight k'. Since $\tilde{f}$ is nonzero, we can write $\tilde{\phi} = \tilde{g}/\tilde{f}$ and while $\tilde{\phi}$ belongs (a-priori) to the field of fractions of $\tilde{M}$, as $\tilde{g}$ and $\tilde{f}$ are modular forms of the same weight we have that $p\tilde{h}i$ must belong to the fraction field of $\tilde{M}^0$. Now we can consider $\tilde{\psi} = \tilde{\phi} - \tilde{\phi}^p$ with

$$\tilde{\psi} = \sum_{(p,n)=1} \sigma_{h-1}(n) q^n \ .$$

One can easily verify that

$$\psi = \theta^{h-1}(\sum_{n=1}^{\infty} \sigma_1(n) q^n)$$

To arrive to the contradiction we note that, as $p = 3$ we have that $\tilde{\psi} = \tilde{\Delta}$, by the congruences of $\tau(n)$ modulo 6. Now $\tilde{M} \cong \mathbb{F}_p[\tilde{\Delta}]$ and the equation $x - x^3 = \tilde{\Delta}$ is irreducible on $\mathbb{F}_p(\tilde{\Delta})$, so we have a contradiction. If $p \geq 5$ one has

$$\tilde{\psi} = -\frac{1}{24}\theta^{h-1}(\tilde{P}) = -\frac{1}{24}\theta^{h-2}(\tilde{E}_{p+1})$$

and hence $\tilde{\psi}$ belongs to $\tilde{M}^0$ by it being integrally closed. We have a filtration on the spaces $\tilde{M}_k$, given by

$$\mathrm{Fil}^i(\tilde{M}_k) = \{f \in \tilde{M}_k | f \equiv f', f' \in \tilde{M}_{k-i(p-1)}\} \ .$$

For $f \in_k$, set $\beta(f) = \min\{i \in \mathbb{N} | f \in \mathrm{Fil}^i(\tilde{M}_k)\}$, then if $\beta(f) = i$, it must be $\beta(\theta f) = (p+1)i$ and therefore $\beta(\tilde{\psi}) = (h-1)p + 1 + p - 1 = h(p+1)$, but as $\psi \in \tilde{M}^0$ it must be $\beta(\tilde{\psi}) = hp$ which is absurd and we are done.

□

Now we can construct the group of weights of $p-$adic modular forms. Consider a cauchy sequence of modular forms $\{f_i\}$ converging to a p-adic modular form f, call w_i the sequence of weights, we have just shown that this sequence is cauchy in the projective limit

$$X = \lim_{\leftarrow} \mathbb{Z}/p^n(p-1)\mathbb{Z} \cong \lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \cong \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z} \ .$$

X is Lie, p-adic and of dimension 1, moreover the canonical morphism $\mathbb{Z} \to X$ is injective and identifies $\mathbb{Z}$ with a dense subgroup of X. We want to see the elements of X as (p-adic) characters on the group $\mathbb{Z}_p^\star$ of p-adic units. More precisely, let V_p be the set of continuous endomorphism of $\mathbb{Z}_p^\star$ endowed with the topology of uniform convergence, then the map $\mathbb{Z} \to V_p$ extends to to a continuous bijection $\epsilon : X \to V_p$ (this only holds for $p \neq 2$).

Denote now the action of an element $k \in X$ on v by v^k. Clearly we can write $k = (s, u)$ where $s \in \mathbb{Z}_p$ and $u \in \mathbb{Z}/(p-1)\mathbb{Z}$ and let $v = v_1 v_2$ where $v_1^{p-1} = 1$ and $v_2 \equiv 1 \bmod p$, then one has $v^k = (v_1 v_2)^k = v_1^k v_2^k = v_1^u v_2^s$. Moreover we can define a concept of being of even weight, considering the torsion part. Namely $k \in X$ will be said to be even if $(-1)^k = 1$ i.e. if and only if $u \in 2\mathbb{Z}/(p-1)\mathbb{Z}$.

3 Modular forms à la Katz

In this section we follow [3, Chapter 2 (parts), Chapter 4]. While Serre's approach to p-adic modular forms revolves more on immediately preserving the q-expansion principle, Katz's point of view is based on the relation between modular forms and elliptic curves, first of all let's recall an (alternative) classical definition of elliptic curve.

Definition 7. an elliptic curve over a scheme S is a triplet (E, p, s) where E is a scheme, $p : E \to S$ is a proper smooth morphism with geometrically connected fibers which are curves of genus 1, and s is a section of p.

Definition 8. With the notation of the above we denote by $\omega_{E/S}$ the sheaf $p_\star(\Omega_{E/S})$ which is canonically isomorphic (by Serre's duality) to the sheaf $R^1 p_\star(\mathcal{O}_E)$.

Now we can define modular forms of level 1, generalizing the classical relation with elliptic curves over the complex numbers.

Definition 9. A level 1 modular form of weight k is a rule f that associates to a couple (E, s) an element $f((E, s)) \in \Gamma(S, (\omega_{E\setminus S})^{\otimes k})$ such that

- f depends only on the isomorphism class of E;
- f commutes with arbitrary base-changes, namely for each base extension $S \xrightarrow{g} S'$, one has $f(E_{S'}/S') = g^\star(f(E/S))$.

We will denote the $\mathbb{Z}$-module of such forms with $M^!(\mathbb{Z}, 1, k)$

Note that in the affine case $S = \operatorname{Spec}(R)$ and $\omega_{E\setminus S}$ free over R with basis ω this definition can be rewritten using the relation

$$f(E/\operatorname{Spec}(R)) = f(E/R, \omega)\omega_{E\setminus S}^{\otimes k}$$

where the right-hand-side makes sense in the meaning of the following

Definition 10. With the notation above a level 1 modular form of weight k is a rule f that associates to a couple $(E/\operatorname{Spec}(R), \omega)$, composed by an elliptic curve E and a basis of its associated sheaf ω, an element $f(E/\operatorname{Spec}(R), \omega) \in R$ such that

- f depends only on the isomorphism class of $(E/\operatorname{Spec}(R), \omega)$
- for each $\lambda \in R^\star$, $f(E, \lambda\omega) = \lambda^{-k} f(E/\operatorname{Spec}(R), \omega)$
- for any $g : R \to R'$ one has $f(E_{R'}/\operatorname{Spec}(R'), \omega_{R'}) = g(f(E/\operatorname{Spec}(R), \omega))$.

If we restrict ourselves to the case of schemes over a fixed ground-ring R_0 we automatically get the notion of modular forms of weight k and level 1 over R_0, the R_0-module of which will be denoted as $M^!(R_0, 1, k)$.

To recover the concept of q expansion we note that a modular form $f \in M^!(R_0, 1, k)$ can always be evaluated on the couple $(\operatorname{Tate}(q), \omega_{\text{can}})$ composed by the Tate curve and the canonical differential on it, considered over the ring $\mathbb{Z}((q)) \otimes_{\mathbb{Z}} R_0$ (note that such is not $R_0((q))$).

Definition 11. Given a modular form $f \in M^!(R_0, 1, k)$ its q-expansion is the finitely-tailed Laurent series $f((\mathrm{Tate}((q)), \omega_{\mathrm{can}})_{R_0}) \in \mathbb{Z}((q)) \otimes_{\mathbb{Z}} R_0$, we will say that f is holomorphic if $f((\mathrm{Tate}((q)), \omega_{\mathrm{can}})_{R_0}) \in \mathbb{Z}[[q]] \otimes_{\mathbb{Z}} R_0$ and we will denote the R_0-module of those forms with $M(R_0, 1, k)$.

Note that $\mathbb{Z}((q)) \otimes_{\mathbb{Z}} R_0 \subset R_0((q))$ so that $f((\mathrm{Tate}((q)), \omega_{\mathrm{can}})_{R_0})$ is a finite R_0-linear combination of elements of $\mathbb{Z}((q))$ (this implies, for example, that if R_0 is the fraction field of a discrete valuation ring, then the q-expansion of f has bounded denominators).

We now want to introduce the concept of modular forms of level n. For any integer $n \geq 1$, we will denote by ${}_nE$ the group-scheme given by the kernel of the multiplication by n endomorphism of E, such group scheme is finite, flat, commutative and of rank n^2 over S and it is étale over S if and only if $n \in \Gamma(S, \mathcal{O}_S)^\star$, id est if and only if S is a scheme over $\mathbb{Z}[\frac{1}{n}]$.

Definition 12. A level n structure on an elliptic curve E over S is an isomorphism

$$\alpha_n : {}_nE \to (\mathbb{Z}/n\mathbb{Z})^2$$

Note that such isomorphism cannot exists if $n \notin \Gamma(S, \mathcal{O}_S)^\star$, conversely, when $n \in \Gamma(S, \mathcal{O}_S)^\star$ it must exists an étale covering S' of S on which $E_{S'}$ admits a level n structure. Moreover, if a E/S admits one level n structure and S is connected, then the set of all level n structure on E is homogeneous principal under $\mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z}) = \mathrm{Aut}((\mathbb{Z}/n\mathbb{Z})^2)$.

Now we can give the following

Definition 13. A modular form of level n and weight k is a rule f that associates to a couple $(E/S, \alpha_n)$ (Where E/S is an elliptic curve and α_n is an level n structure on it) an element $f(E/S, \alpha_n) \in \Gamma(S, \omega_{E/S}^{\otimes k})$ which commutes with arbitrary base change. Using the identification as before we can define $M^!(R_0, n, k)$.

If f is a modular form of level n and weight k over the ground ring R_0 and both $\frac{1}{n}, \zeta_n \in R_0$ we can evaluate f on the triplet $(\mathrm{Tate}(q^n), \omega_{\mathrm{can}}, \alpha_n)_{R_0}$ composed by the Tate curve, its canonic differential and any level n structure, all defined over $\mathbb{Z}((q)) \otimes R_0$ (Note that all the points of ${}_n\mathrm{Tate}(q^n)$ are rational over $\mathbb{Z}((q)) \otimes R_0$ as those are the canonical images of $\zeta_n^i q^j$ for $\mathbb{G}_m$ and therefore they lie in $\mathbb{Z}((q)) \otimes \mathbb{Z}[\zeta_n, \frac{1}{n}]$. One can also show that the non-constant q-coefficients of their (x,y)-coordinates lie in $\mathbb{Z}[\zeta_n]$ by the Jacobi-Tate formulas).

Using this fact we can again define the q-expansions of f as the finitely-tailed Laurent series $f((\mathrm{Tate}(q^n), \omega_{\mathrm{can}}, \alpha_n)_{R_0}) \in \mathbb{Z}((q)) \otimes R_0$ obtained by varying the level structure α_n. One can immediately notice that, while it makes sense to talk about modular forms of level n for any ring R_0, we can define its q-expansion only if $\zeta_n, \frac{1}{n} \in R_0$.

Definition 14. A modular form f of level n and weight k is said to be holomorphic at ∞ if its base-change on $R_0[\frac{1}{n}, \zeta_n]$ has all q-expansions in $\mathbb{Z}[[q]] \otimes R_0[\zeta_n, \frac{1}{n}]$.

Definition 15. Using the same approach we call a modular form of weight k and level n for $\Gamma_0(p)$ a law that associates to a quadruple (E, s, α_n, H) where the new object H is a finite, flat subgroup-scheme of E of rank p an element $f(E, s, \alpha_n, H) \in \Gamma(S, \omega_{E/S}^{\otimes k})$ such that, as always, this assignation depends only on the isomorphism class of the quadruple and it commutes with arbitrary base-changes.

When we have that $\zeta_n, \frac{1}{n} \in R_0$, we can make sense of a concept of q-expansion also for those modular form by evaluating f on the usual triplet where we add a canonical subgroup of E of rank p. More precisely we have the following

Definition 16. Let f be a modular form of level n and weight k for $\Gamma_0(p)$ for some prime p, then we call "the q-expansion of f at the unramified cusps" the finitely-tailed Laurent series $f((\mathrm{Tate}(q^n), \omega_{\mathrm{can}}, \alpha_n, \mu_p)_{R_0})$ obtained by varying the level n structure α_n. Analogously we call "the q-expansion of f at the ramified cusps" the finitely-tailed Laurent series $f((\mathrm{Tate}(q^{np}), \omega_{\mathrm{can}}, \alpha_n, \{q^n\})_{R_0})$, where $\{q^n\}$ is the rank p flat subgroup-scheme of the Tate curve generated by (the image of) q^n.

We say that f is holomorphic if all its q-expansions lie in $\mathbb{Z}[[q]] \otimes R_0$.

For $n \geq 3$ one has that the functor that associates to a scheme the isomorphism classes of elliptic curves over such scheme endowed with level n structure is representable. It is represented by M_n which is an affine smooth curve over $\mathbb{Z}[\frac{1}{n}]$. Such is finite and flat of degree equal to the cardinality of $\mathrm{PGL}_2(\mathbb{Z}/n\mathbb{Z})$ over the j-line $\mathbb{Z}[j, \frac{1}{n}]$ and it's étale on the open set of the affine j-line where j and $j - 1728$ are invertible. The normalization of the projective j-line $\mathbb{P}^1_{\mathbb{Z}[\frac{1}{n}]}$ in M_n is a proper and smooth curve $\bar{M}_n$ over $\mathbb{Z}[\frac{1}{n}]$, and $\Gamma(\bar{M}_n, \mathcal{O}_{\bar{M}_n}) \cong \mathbb{Z}[\zeta_n, \frac{1}{n}]$. The curve $M_n \otimes_{\mathbb{Z}[\frac{1}{n}]} \mathbb{Z}[\frac{1}{n}, \zeta_n]$ (respectively $\bar{M}_n \otimes_{\mathbb{Z}[\frac{1}{n}]} \mathbb{Z}[\frac{1}{n}, \zeta_n]$) is a disjoint union of $\varphi(n)$ affine (respectively proper) smooth and geometrically connected curves over $\mathbb{Z}[\frac{1}{n}, \zeta_n]$ where the partition is given by the $\varphi(n)$ n-th roots of unity occurring as values of the Weil pairing on the basis of ${}_nE$ specified by the level n structure.

The scheme $\bar{M}_n \setminus M_n$ is finite and étale over $\mathbb{Z}[\frac{1}{n}]$ and, over $\mathbb{Z}[\zeta_n, \frac{1}{n}]$, is a disjoint union of schemes, called the cusps of $\bar{M}_n$, which are in a natural way the set of isomorphism classes of the Tate curve $\mathrm{Tate}(q^n)$ viewed over $\mathbb{Z}((q)) \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_n, \frac{1}{n}]$. The completion of $\bar{M}_n \otimes \mathbb{Z}[\zeta_n, \frac{1}{n}]$ along any of the cusp is isomorphic to $\mathbb{Z}[\zeta_n, \frac{1}{n}][[q]$ and the completion of the projective j-line $\mathbb{P}^1_{\mathbb{Z}[\zeta_n, \frac{1}{n}]}$ along ∞ is itself isomorphic to $\mathbb{Z}[\zeta_n, \frac{1}{n}][[q]]$ via the formula

$$j(\mathrm{Tate}(q)) = \frac{1}{q} + 744 + \dots \ .$$

The endomorphism of $\mathbb{Z}[\zeta_n, \frac{1}{n}][[q]]$ arising from the projection $\bar{M}_n \to \mathbb{P}^1$ is just given by $q \mapsto q^n$. In fact, for each cusp, the inverse image of the universal elliptic curve with level n structure $(E/M_n, \alpha_n)$ over (the spectrum of) $\mathbb{Z}[\zeta_n, \frac{1}{n}]$

(viewed as a punctured disc around the cusp) is isomorphic to the inverse image over $\mathbb{Z}[\zeta_n, \frac{1}{n}]((q))$ of the Tate curve $\mathrm{Tate}(q^n)$ with the level n structure corresponding to that cusp.

There is a unique invertible sheaf ω on $\bar{M}_n$ whose restriction to M_n is ω_{E/M_n} (where $(E/M_n, \alpha_n)$ is the universal elliptic curve with level n structure), and whose sections over the completion $\mathbb{Z}[\zeta_n, \frac{1}{n}][[q]]$ at each cusp are precisely the $\mathbb{Z}[\zeta_n, \frac{1}{n}][[q]]$-multiples of the canonical differential of the Tate curve. The Kodaira-Spencer style of isomorphism

$$(\omega_{E/M_n})^{\otimes 2} \cong \Omega^1_{M_n/\mathbb{Z}[\frac{1}{n}]}$$

extends to an isomorphism

$$(\omega)^{\otimes 2} \cong \Omega^1_{M_n/\mathbb{Z}[\frac{1}{n}]}(\log(\bar{M}_n - M_n))$$

and in fact, over $\mathbb{Z}[\frac{1}{n}][[q]]$, the "square" of the canonical differential ω_{can} of $\mathrm{Tate}(q^n)$ corresponds to $n\frac{dq}{q}$.

Example 1. Consider the complex case, and let $\sigma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, then we compute $\frac{d(\sigma z)}{dz}$.

$$\frac{d(\sigma z)}{dz} = \frac{d(\frac{az+b}{cz+d})}{dz} = \frac{-c(az+b)+a(cz+d)}{(cz+d)^2} = \frac{ad-bc}{(cz+d)^2} = (cz+d)^{-2}$$

hence, if $f \in M^!(1,2)$ (one can take $f = E_2$, to be even more concrete), the differential defined by $f(z)dz$ is invariant by the action of σ, as we have

$$f(\sigma z)d(\sigma z) = (cz+d)^2 f(z)(cz+d)^{-2}dz = f(z)dz \ .$$

It follows that a modular form of level n and weight k, holomorphic at ∞ and defined over any ring R_0 where n is invertible is just a section of $(\omega)^{\otimes k}$ on $\bar{M}_n \otimes_{\mathbb{Z}[\frac{1}{n}]} R_0$, or equivalently a section of the quasi-coherent sheaf $(\omega)^{\otimes k} \otimes_{\mathbb{Z}[\frac{1}{n}]} R_0$ on $\bar{M}_n$

3.1 The q-expansion principle

Definition 17. Given a $\mathbb{Z}[\frac{1}{n}]$ module K, a modular form of level n and weight k holomorphic at ∞, with coefficients in K is an element of $H^0(\bar{M}_n, (\omega)^{\otimes k} \otimes_{\mathbb{Z}[\frac{1}{n}]} K)$. At each cusp, such modular form has q-expansion in $K \otimes_{\mathbb{Z}[\frac{1}{n}]} \mathbb{Z}[\zeta_n, \frac{1}{n}] \otimes_{\mathbb{Z}} \mathbb{Z}[[q]]$.

Theorem 5. *Let $n \geq 3$ and let K be a $\mathbb{Z}[\frac{1}{n}]$-module, f a modular form of level n and weight k. Suppose that on each of the $\varphi(n)$ components of $\bar{M}_n \otimes_{\mathbb{Z}[\frac{1}{n}]} \mathbb{Z}[\zeta_n, \frac{1}{n}]$, there is at least one cusp at which the q-expansion of f vanishes identically, then $f = 0$.*

Before we prove this theorem, let us state the main corollary:

Corollary 1. (q-expansion principle) Let $n \geq 3$, K a $\mathbb{Z}[\frac{1}{n}]$-module, let L be a submodule of K and suppose that f is a modular form of level n and weight k, holomorphic at ∞ with coefficients in K. If on each of the $\varphi(n)$ connected components of $\bar{M}_n \otimes_{\mathbb{Z}[\frac{1}{n}]} \mathbb{Z}[\zeta_n, \frac{1}{n}]$ there is at least one cusp at which all the coefficients of f lie in $L \otimes_{\mathbb{Z}[\frac{1}{n}]} \mathbb{Z}[\zeta_n, \frac{1}{n}]$, then f is a modular form with coefficients in L.

Proof. (of corollary)

As L is a submodule of K we have the short exact sequence

$$0 \to L \to K \to K/L \to 0$$

which gives us the exact sequence of sheaves

$$0 \to L \otimes (\omega)^{\otimes k} \to K \otimes (\omega)^{\otimes k} \to K/L \otimes (\omega)^{\otimes k} \to 0$$

and hence we get, in cohomology

$$0 \to H^0(\bar{M}_n, L \otimes (\omega)^{\otimes k}) \to H^0(\bar{M}_n, K \otimes (\omega)^{\otimes k}) \to H^0(\bar{M}_n, K/L \otimes (\omega)^{\otimes k}).$$

If we now apply the theorem to the image of f in $H^0(\bar{M}_n, K/L \otimes (\omega)^{\otimes k})$ we deduce the thesis by the exactness of the cohomology sequence.

□

Proof. (of Theorem)

By passing to the ring of dual numbers $D(K) = \mathbb{Z}[\frac{1}{n}] \oplus K$ we may assume that K is a ring over $\mathbb{Z}[\frac{1}{n}]$, furthermore, as cohomology of quasi-coherent sheaves commutes with inductive limits we may assume that K is finitely generated and then that K is local and noetherian. Since taking completion is faithfully flat, we can now reduce to the case where K is a local and complete noetherian ring and by Grothendieck's comparison theorem for cohomology and quotients that is artinian and local.

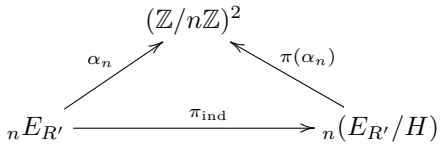
By Krull's intersection theorem f induces the 0-section of $(\omega)^{\otimes k}$ over an open neighborhood of a cusp on each connected component of $\bar{M}_n \otimes K \otimes \mathbb{Z}[\zeta_n, \frac{1}{n}]$ hence a open and dense subset of $\bar{M}_k \otimes K$. If f is non zero, it exists a non-void closed subset Z of $\bar{M}_k \otimes K$, containing no maximal points of $\bar{M}_k \otimes K$ (by density), on which f is supported. Over the local ring in $\bar{M}_k \otimes K$ of any maximal point z of Z f becomes non-canonically a section of $\mathcal{O}_{\bar{M}_k \otimes K, z}$ which is supported on the closed point, id est, for any $g \in \mathfrak{m}_z \subset \mathcal{O}_{\bar{M}_k \otimes K, z}$ it exists an m such that $g^m f = 0$ and therefore any element of $\mathfrak{m}_z$ is a zero-divisor, meaning that z is a point of depth 0. As $\bar{M}_n \otimes K$ is smooth over K which is artinian and local and hence is Cohen-Macaulay, which implies that only maximal points have depth 0, thus z is maximal in $\bar{M}_n \otimes K$ and we have a contradiction, so that f must be 0.

□

3.2 Hecke Operators

We now want to recover a notion of Hecke operators for our newly-built modular forms. To do so we start with a prime l which is invertible in our base ring R and doesn't divide the level n of our modular form. Under those hypothesis the subgroups scheme ${}_lE$ of an elliptic curve E defined over R is finite and étale, moreover it exists an étale cover R' on which ${}_lE$ is (non-canonically) isomorphic to $(\mathbb{Z}/l\mathbb{Z})^2$, thus $E_{R'}$ has $l+1$ finite and flat subgroup-schemes or rank l. Let H be one of those, $\pi : E_{R'} \to E_{R'}/H$ be the projection map and $\check{\pi} : E_{R'}/H \to E_{R'}$ be its dual (which is still étale and of degree l). Then we have that $\pi \circ \check{\pi} = l\cdot$ on $E_{R'}/H$ and $\check{\pi} \circ \pi = l\cdot$ on $E_{R'}$.

If ω is a non-vanishing differential on E_R then $\check{\pi}^\star(\omega_{R'}) = \mathrm{Tr}_\pi(\omega_{R'})$ is a never-vanishing differential over $E_{R'}/H$. Let $\alpha_n :_n E \to (\mathbb{Z}/n\mathbb{Z})^2$ be a level n structure on E/R, then it exists a unique level n structure $\pi(\alpha_n)$ on $E_{R'}$ such that the following diagram commutes



Given a modular form of level n and weight k with coefficients in R , for each triplet (E, ω, α_n) we can consider the sum

$$\sum_H f((E_{R'}, \check{\pi}^\star(\omega), \pi(\alpha_n)))$$

(such lies in R and is independent by the choice of the étale covering R'). Normalizing the sum by a factor l^{k-1} we get

$$(T_l f)(E, \omega, \alpha_n) := l^{k-1} \sum_H f((E_{R'}, \check{\pi}^\star, \pi(\alpha_n)))$$

as definition of the Hecke operator T_l.

We can ask ourselves how the operator T_l acts on the q-expansion of f. The l-division points of the Tate curve $\mathrm{Tate}(q^n)$ over $\mathbb{Z}((q)) \otimes_{\mathbb{Z}} \mathbb{Z}[\frac{1}{nl}]$ become rational over $\mathbb{Z}((q^{1/l})) \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_{nl}, \frac{1}{nl}]$ and we can now identify the $l+1$ subgroup as

$$\begin{cases} \mu_l = \langle \zeta_l \rangle \\ H_i = \langle (\zeta_l^i q^{1/l})^n \rangle \quad \text{for } i = 0, 1, \ldots, l-1 \ . \end{cases}$$

For the subgroup μ_l, the quotient $\mathrm{Tate}(q^n)/\mu_l$ is $\mathrm{Tate}(q^{nl})$ and the dual isogeny consists on dividing $\mathrm{Tate}(q^{nl})$ by the subgroup generated by q^l. The isomorphism is obtained by the extension of scalars $\phi_l : \mathbb{Z}((q)) \to \mathbb{Z}((q))$ defined by $q \mapsto q^l$.

For the subgroups H_i the quotient $\mathrm{Tate}(q^n)/H_i$ is $\mathrm{Tate}((\zeta_l^i q^{\frac{1}{l}})^n)$ and the dual isogeny consists in dividing the curve by its own subgroup μ_l. Here the isomorphisms are given (over $\mathbb{Z}[\zeta_{nl}, \frac{1}{nl}]$) by the scalar extensions $\phi_i : \mathbb{Z}[\zeta_{nl}, \frac{1}{nl}]((q^{\frac{1}{l}})) \to \phi_i : \mathbb{Z}[\zeta_{nl}, \frac{1}{nl}]((q^{\frac{1}{l}}))$ defined via $q^{\frac{1}{l}} \mapsto \zeta_l^i q^{\frac{1}{l}}$

Thus, for μ_l we have that $\check{\pi}^\star(\omega_{\mathrm{can}}) = \omega_{\mathrm{can}}$ on $\mathrm{Tate}(q^{nl})$ and for the H_i $\check{\pi}^\star(\omega_{\mathrm{can}}) = l(\omega_{\mathrm{can}})$ on $\mathrm{Tate}((\zeta_l^i q^{\frac{1}{l}})^n)$. Denote with α'_n the unique level n structure on $\mathrm{Tate}(q^n)$ such that $\phi_l^\star(\alpha'_n) = \pi_l(\alpha_n)$ (where $\pi_l(\alpha_n)$ is the image of the level n structure α_n under the projection map). We have

$$\begin{aligned} f((\mathrm{Tate}(q^n)/\mu_l, \check{\pi}^\star(\omega_{\mathrm{can}}), \pi_l(\alpha_n))) &= f((\mathrm{Tate}(q^{nl}, \omega_{\mathrm{can}}, \phi_l^\star(\alpha'_n)))) \\ &= \phi_l(f((\mathrm{Tate}(q^n), \omega_{\mathrm{can}}, \alpha'_n))). \end{aligned}$$

To do the same for the H_i we denote with π_i the projection and then we get immediately the relation $\pi_i(\alpha_n) = \phi_i^\star(\pi_0(\alpha_n))$. Call α''_n the level n structure $i_l^\star(\pi_0(\alpha_n))$ on $\mathrm{Tate}(q^{\frac{n}{l}})$ obtained by the scalar extension (which is actually a ring isomorphism) $i_l : \mathbb{Z}[\zeta_{nl}, \frac{1}{nl}]((q^{\frac{1}{l}})) \to \mathbb{Z}[\zeta_{nl}, \frac{1}{nl}]((q))$ defined by $q^{\frac{1}{l}} \mapsto q$. We get

$$\begin{aligned} f((\mathrm{Tate}(q^n)/H_i, \check{\pi_i}^\star(\omega_{\mathrm{can}}), \pi_i(\alpha_n))) &= f((\mathrm{Tate}((\zeta_l^i q^{\frac{1}{l}})^n), l\omega_{\mathrm{can}}, \pi_0(\alpha_n))) \\ &= \phi_i(f((\mathrm{Tate}(q^{\frac{n}{l}}), l\omega_{\mathrm{can}}, \pi_0(\alpha_n)))) \\ &= \phi_i \circ (i_l)^{-1}(f((\mathrm{Tate}(q^n), \omega_{\mathrm{can}}, \alpha''_n))) \\ &= \frac{1}{l}\phi_i \circ (i_l)^{-1}(f((\mathrm{Tate}(q^n), \omega_{\mathrm{can}}, \alpha''_n)). \end{aligned}$$

From those we get a formula for T_l. Let f be a modular form of weight k and level n with coefficients in R, and let l be a prime not dividing n, invertible in R. Then suppose the q-expansion of f is given by

$$f(\mathrm{Tate}(q^n), \omega_{\mathrm{can}}, \alpha_n) = \sum_{i > -\infty} a_i(\alpha_n) q^i$$

Then we have, form what we have said,

$$(T_l f)(\mathrm{Tate}(q^n), \omega_{\mathrm{can}}, \alpha_n) = \sum_{i > -\infty} b_i(\alpha_n) q^i$$

where the b_i are defined by the formula

$$b_i(\alpha_n) = l^{k-1} a_{\frac{i}{l}}(\alpha'_n) + a_{li}(\alpha''_n)$$

with the usual convention that $a_{\frac{i}{l}}(\alpha'_n) = 0$ when $l \nmid i$.

Form the formula we immediately get the following

Corollary 2. The operator T_l maps modular forms holomorpic at ∞ in modular forms holomorphic at ∞ and cuspidal forms in cuspidal forms.

To convince ourselves that this definition of Hecke operators makes sense (if still needed) we have a nice proposition

Proposition 1. *Let $n \geq 2$ and $k \geq 2$. Given a prime $l \nmid n$ and any $\mathbb{Z}[\frac{1}{n}]$ − module K it exists one and one only endomorphism of $M(K, n, k)$ which action on the q-expansions is given by the formula above.*

Proof. By base-change we can assume $K = \mathbb{Z}[\frac{1}{n}]$ and given a modular form with coefficients in $\mathbb{Z}[\frac{1}{n}]$, while $(T_l f)$ has a-priori coefficients in $\mathbb{Z}[\frac{1}{nl}]$ those must lie in $\mathbb{Z}[\zeta_n, \frac{1}{n}]$. Uniqueness is obvious

□

Corollary 3. Let $k \geq 2$, given any l and any $\mathbb{Z}$-module K it exists a unique endomorphism of $S(K, 1, k)$ whose effect on the q-expansion is given by the previous formulas.

Proof. Let us choose $n, m \geq 3$ such that n, m, l are all prime one to the other we can recover $H^0(\bar{M}_n, \omega^{\otimes k} \otimes (K \otimes \mathbb{Z}))$ as the pull-back of the diagram

$$\begin{array}{ccc} H^0(\bar{M}_n, \omega^{\otimes k} \otimes (K \otimes \mathbb{Z}[\frac{1}{n}])) & & \\ & \searrow & \\ & & H^0(\bar{M}_{mn}, \omega^{\otimes k} \otimes (K \otimes \mathbb{Z}[\frac{1}{mn}])) \\ & \nearrow & \\ H^0(\bar{M}_m, \omega^{\otimes k} \otimes (K \otimes \mathbb{Z}[\frac{1}{m}])) & & \end{array}$$

Therefore we get T_l for the forms of level 1 by considering the operator defined uniquely by this fibered product, which we just constructed for the spaces of level n, m and nm. □

3.3 The Hasse invariant as a modular form

Let R be an $\mathbb{F}_p$-algebra and let E be an elliptic curve over R. The absolute Frobenius map F_{abs} is a p-linear additive endomorphism of $\mathcal{O}_E$ and therefore induces a p-linear endomorphism on the R-module $H^1(E, \mathcal{O}_E)$. Let ω be a basis of $\omega_{E/R}$, such determines the dual basis η of $H^1(E, \mathcal{O}_E)$ and define the Hasse invariant $A(E, \omega)$ as the number that realizes the identity

$$F^\star_{\text{abs}}(\eta) = A(E, \omega)\eta$$

Now we can immediately notice that passing form ω to $\lambda\omega$ (for $\lambda \in R^\star$) induces the transformation $\eta \mapsto \frac{1}{\lambda}\eta$ at the level of dual basis. If now we apply $F^\star_{\text{abs}}$ we have

$$F^\star_{\text{abs}}(\lambda^{-1}\eta) = \lambda^{-p} F^\star_{\text{abs}}(\eta) = \lambda^{-p} A(E, \omega)\eta = \lambda^{1-p} A(E, \omega)\lambda^{-1}\eta = \lambda^{1-p} A(E, \omega) \ .$$

Which shows that the Hasse invariant A is a modular form of level 1 and weight $p - 1$ with coefficients in $\mathbb{F}_p$.

With more intrinsic point of view one can look at $F^\star_{abs}$ as the R-linear homomorphism

$$F^\star_{\text{abs}} : (H^1(E, \mathcal{O}_E))^{\otimes p} \to H^1(E, \mathcal{O}_E)$$

and therefore as a section of $(\omega_{E/R})^{\otimes p-1}$ (as we have $\text{Hom}((H^1(E, \mathcal{O}_E))^{\otimes p}, H^1(E, \mathcal{O}_E)) \cong \text{Hom}((H^1(E, \mathcal{O}_E))^{\otimes p} \otimes (H^1(E, \mathcal{O}_E))^{\otimes -1}, \mathcal{O}_E)$. In terms of ω, this section is $A(E, \omega)\omega^{\otimes p-1}$. To notice that A is holomorphic at ∞ one can see that the Tate

curve over $\mathbb{F}_p((q))$ is the restriction of a plane curve C defined over $\mathbb{F}_p[[q]]$ and its canonic differential ω_{can} is the restriction to a basis over $\mathbb{F}_p[[q]]$ of the dualizing sheaf of C. Hence ω_{can} defines the dual basis η_{can} of $H^1(C, \mathcal{O}_C)$ as $\mathbb{F}_p[[q]]$-module and $A(\mathrm{Tate}(q), \omega_{\mathrm{can}})$ is the representative matrix of $F^{\star}_{\mathrm{abs}}$ on $H^1(C, \mathcal{O}_C)$ with respect to η. In particular we have $A(\mathrm{Tate}(q), \omega_{\mathrm{can}}) \in \mathbb{F}_p[[q]]$. An alternative way to get holomorpy at ∞ comes form the following fact: if E/R is an elliptic curve $H^1(E, \mathcal{O}_E)$ is the tangent space of E in the origin, which is the R-module of all the derivations which are invariant under the translations of E/R. As R is an algebra over $\mathbb{F}_p$ the action of $F^{\star}_{\mathrm{abs}}$ on $H^1(E, \mathcal{O}_E)$ consists in taking the p-th iterate of an invariant derivation. Now we utilize the existence of a local parameter t on the completion of the Tate curve along the identity section in terms of which $\omega_{\mathrm{can}} = \frac{dt}{t+1}$. Let D be the invariant derivation obtained as dual of ω_{can}, then $D(t) = 1 + t$ and therefore it must be $D(1 + t) = D(D(t)) = 1 + t$ so that $D^n(t) = 1 + t$ for all $n \geq 1$. Over $\mathbb{F}_p$ D^p is an invariant derivation and coincides with D on ω_{can}, thus $D^p = D$, leading us to $F^{\star}_{\mathrm{abs}}(\eta) = \eta$ and hence $A(\mathrm{Tate}(q), \omega_{\mathrm{can}}) = 1$.

4 p-adic modular forms à la Katz and the relation with Serre's definition

Let $q = p^r$, call $W_N(K)$ the ring of Witt vectors of length N over a perfect field $K \subset \mathbb{F}_q$ and let S_N be a flat, affine scheme with normal, irreducible and reduced generic fiber defined over $W_N(K)$. Furthermore we assume that S_N admits an endomorphism φ which induces the q-th power map on the special fiber. Note that such is always true if S_N is affine and smooth.

Theorem 6. *We have an equivalence between the category of free, finite $W_n(K)$-modules with a continuous action of $\pi_1^{\acute{e}t}(S_N)$ (Note that those are representations of $\pi_1^{\acute{e}t}(S_N)$ on the ring of Witt vectors endowed with the discrete topology) and the category of the couples (H, F) formed by a locally free sheaf H of finite rank on S_N and an isomorphism $F : \varphi^\star(H) \to H$.*

Proof. Given a representation M of $\pi_1^{\text{ét}}(S_N)$, let T_N be a finite and étale S_N-scheme such that the representation factors through $\mathrm{Aut}(T_N/S_N)$ (as such is finite). As T_N is étale over S_N there is a unique φ-linear endomorphism which induces the q-th power endomorphism of $T_N \times_{W_N(K)} K$, let us call it φ_T. By uniqueness φ_T commutes with the action of $\mathrm{Aut}(T_N/S_N)$, let then H_T be the T_n-module $M \otimes_{W_N(\mathbb{F}_q)} \mathcal{O}_{T_N}$ and let F_T be the φ_T-linear endomorphism of H_T defined by $F_T(m \otimes f) = m \otimes \varphi_T(f)$. For g any automorphism of S_N we can define an action of $\mathrm{Aut}(T_N/S_N)$ on (H_T, F_T) by setting $g(m \otimes f) = g(m) \otimes (g^{-1})^\star(f)$. By descent we have a one to one correspondence between $\mathrm{Aut}(T_N/S_N)$-equivariant sheaves on T_N (and the corresponding map) and sheaves on S_N. Therefore it exists a unique couple (H, F) defined on S_N such that its inverse image on T_N is $\mathrm{Aut}(T_N/S_N)$-isomorphic to (H_T, F_T).

The rule $M \mapsto (H, F)$ defines a functor, that we will prove give us the equivalence in the theorem. Notice that we can recover M as the fixed points of F_T acting on the module of global sections H_T as a φ-linear endomorphism, so that our functor is fully faithful. What is left to (not effortlessly) show in order to get the equivalence is that each (H, F) arises in this way. More concretely we must now prove that given any (H, F), there exists a finite and étale covering T_N of S_N over which H admits a basis of F-Fixed points.

Suppose $N = 1$. Then $S_1 = S$ is a scheme over K and (H, F) is a couple composed by a locally free S-module H of finite rank and a φ-linear endomorphism of H which induces an isomorphism $F : H^{(q)} \to H$. Given any S-scheme T call H_T the inverse image of H on T and $F_T : H_T^{(q)} \to H_T$ the induced morphism.

Recall that the functors of S-schemes

$$X(T) = \text{ global sections of } H_T$$

$$Y(T) = \text{ bases of } H_T$$

$$Z(T) = \text{ bases of } H_T \text{ consisting of } F_T\text{-fixed points}$$

are all representable, the first by $\mathrm{Spec}_S(\mathrm{Symm}(\check{H})$ see [1, 9.4.4,9.4.5], to have an idea of why note that S is affine and we may assume that $H \cong e_1\mathcal{O}_S \oplus \cdots \oplus e_r\mathcal{O}_S$ so that $\mathrm{Symm}(H) \cong \mathcal{O}_S[\check{e}_1, \ldots, \check{e}_r]$ and give a T-point of is relative spectrum is just to give an r-uple of scalars t_i of $\mathcal{O}_T(T)$ which defines the element $t_1e_1 + \ldots t_re_r$. The second by the open subset of the $r = \mathrm{rank}(H)$-fold product $X^{r/S} = X \times_S X \times_S \cdots \times_S X$ over which the map $(\mathcal{O}_{X^{r/S}}) \to H_{X^{r/S}}$ is an isomorphism, the third by the closed subscheme of Y over which the universal basis is fixed by F_Y.

We must show that Z is finite and étale over S. As this problem is local on S we may assume that H is free and S is affine. Let $h_1, \ldots, h_r$ be a basis of H and let (a_{ij}) be the invertible matrix obtained by F writing

$$F(h_i) = \sum a_{ji}h_j \ .$$

Consider the functor of S-schemes $Y'(T) =$ sections of H_T fixed by F_T. Such is representable by a finite and étale scheme of rank q^r over S, because a section $\sum X_ih_i$ of H is fixed if and only if $\sum X_jH_j = \sum_i (X_i)^q \sum a_{ji}h_j$, thus Y' is the closed subscheme of $\mathbb{A}^r_S$ defined by the equations

$$X_j = \sum_i a_{ji}(X_i)^q \text{ for } j = 1, \ldots, r \ .$$

Since the matrix (a_{ij}) is invertible, if we denote by (b_{ij}) its inverse, the equations can be rewritten as

$$(X_i)^q = \sum_j b_{ij}X_j \text{ for } j = 1, \ldots, r \ ,$$

which define a finite étale S-scheme of rank q^r.

The scheme Z is the open subscheme of $Y'^{(r/S)}$ where the universal r-tuple of F-fixed sections forms a base of H, hence Z is étale over S.

We now want to show that Z is proper over S. By the valutative criterion, we must show that for any valuation ring V over S, any F-fixed basis of H_k (where k is the fraction field of V) extends to a F-fixed basis of H_V. Since the scheme Y' of fixed points is finite over S, each basis element extends uniquely to a F-fixed section of H_V. To see that the associated map $V^r \to H_V$ is an isomorphism we can look at its determinant, thus reducing ourselves to the case where H_V is of rank 1. Now the matrix of F is just given by $F(h_1) = ah_1$ for some invertible element a of V, and a F-fixed basis of H_k is a vector λh_1, with $\lambda \in k$, satisfying $\lambda = a\lambda^p$. As a is in V, such λ must also be an element of V, so that λh_1 "is" a F-fixed basis of H_V.

To finish the base of this induction we have now left to prove that Z is not empty. As the construction of Z commutes with base changes we can reduce to the case in which $S = \mathrm{Spec}(L)$ for some algebraically closed field L. We note that a finite dimensional vector space over an algebraically closed field with a q-linear automorphism is always generated by is fixed points (see appendix, B) and the set of fixed bases is a $\mathrm{GL}_r(\mathbb{F}_q)$-torsor. Thus Z is finite, étale, of rank

$= \#\,\mathrm{GL}_r(\mathbb{F}_q)$ over S and the action of $\mathrm{GL}_r(\mathbb{F}_q)$ on Z (induced by its action on the F-fixed basis) makes Z itself not a $\mathrm{GL}_r(\mathbb{F}_q)_S$-torsor. The cohomology class of this torsor is an element into $H^1_{\text{ét}}(S, \mathrm{GL}_r(\mathbb{F}_q)) = \mathrm{Hom}(\pi_1^{\text{ét}}(S), \mathrm{GL}_r(\mathbb{F}_q))$ which is (at last) the desired representation.

Now that the basis of the induction is done, we can now move to the inductive step.

Suppose the result known for $N-1$. Then we have a finite étale covering T_{N-1} of $S_{N-1} = S_N \times_{W_N(K)} W_{N-1}(K)$ on which $H/p^{N-1}H$ admits a basis of F-fixed points. There is a unique finite étale covering T_N of S_N such that $T_N \times_{S_N} S_{N-1}$ is T_{N-1}, and replacing S_N by T_n we may assume that $H/p^{N-1}H$ admits a basis of F-fixed points. Let $h_1, \dots, h_r$ be a basis of H which lifts to an F-fixed basis of $H/p^{N-1}H$ (remember that S_N is affine). If we write w for the column vector whose entries are the h_i, we have

$$F(w) = (1 + p^{N-1}\Delta)w \ .$$

In order for $(1 + p^{N-1}C)w$ to be an F-fixed basis we must have

$$(1 + p^{N-1}\varphi(C))(1 + p^{N-1}\Delta)w = (1 + p^{N-1}C)w \ .$$

Which is equivalent to

$$\varphi(C) + \Delta \equiv_p C$$

as S_N is flat over $W_N(K)$. This is a set of r^2 Artin-Schreier equations

$$(c_{ij})^q - c_{ij} = -\Delta_{ij}$$

over $S_1 = S_N \times_{W_N(K)} K$ and on a finite étale cover T_1 of S_1 those admits solution, and therefore on the unique étale covering T_N of S_N such that

$$T_N \times_{S_N} S_1 = T_1$$

the module H_{T_N} admits a F-fixed basis.

□

As S_1 is normal, reduced and irreducible a representation of $\pi_1^{\text{ét}}(S_M) = \pi_1^{\text{ét}}(S_1)$ is just a suitable representation of the Galois group of the function field of S_1 which is unramified outside a fixed set of places. Thus if we take a nonempty open $U \subset S_N$ the restriction functor $\mathcal{R}ep(\pi_1^{\text{ét}}(S_N)) \to \mathcal{R}ep(\pi_1^{\text{ét}}(U))$ is full and faithful, and therefore the equivalent functor $(H, F)_{S_N} \to (H, F)_U$ is fully faithful too.

Let now $p \geq 3$ a prime not dividing n and q a power of p congruent to 1 modulo n. Let us now fix an isomorphism $\mu_n \to \mathbb{Z}/n\mathbb{Z}$ over $W(\mathbb{F}_q)$ (i.e. we choose a primitive n-th root of unity ζ) and let S_N^ζ (respectively $\bar{S}_N^\zeta$) the open subset of $M_n \otimes W_N(\mathbb{F}_q)$ (respectively of $\bar{M}_n \otimes W_N(\mathbb{F}_q)$) where the following conditions hold:

- the Eisenstein series E_{p-1} is invertible;

- the Weil pairing of the basis of ${}_nE$ has value ζ (which means that $\det(\alpha_n)$ is the chosen isomorphism).

The schemes S_N^ζ (respectively $\bar{S}_N^\zeta$) are smooth and affine (respectively proper) over $W_N(\mathbb{F}_q)$ with geometrically connected fibers. One has

$$M_n(W_N(\mathbb{F}_q),1) = \bigcup_{\zeta \text{ primitive}} S_N^\zeta$$

and the analogue identity holds for the projective closures.

Let σ be the Frobenius endomorphism of $W_N(\mathbb{F}_q)$, we have $\sigma(\zeta) = \zeta^p$ and therefore $S_N^{\zeta^p} = (S_N^\zeta)^{(\sigma)}$. The endomorphism ϕ of $\bar{M}_n(W_N(\mathbb{F}_q),1)$ defined by the quotient by the canonical subgroup doesn't preserve the S_N^ζ but sends S_N^ζ in $S_N^{\zeta^p}$ (modulo p the canonical subgroup is just the kernel of the absolute Frobenius morphism). As we noticed $S_N^\zeta \cong (S_N^\zeta)^{(\sigma)}$ we can look at ϕ like a σ-linear endomorphism of each S_N^ζ which, modulo p, induces the p-th power map. Analogously, the endomorphism ϕ of the invertible sheaf $\omega^{\otimes k}$ on $\bar{M}_n(W_N(\mathbb{F}_q),1)$ defined by

$$\phi(f)(E,\omega,\alpha_n) = f(E/H, \check{\pi}^\star(\omega), \pi(\alpha_n))$$

where H is the canonical subgroup can be seen as a ϕ-linear endomorphism of $\omega^{\otimes k}_{|_{\bar{S}_N^\zeta}}$ for each primitive root of unity ζ.

Note that $\omega^{\otimes k}$ is generated by $\phi(\omega^{\otimes k})$ as sheaf; given a local section f of $\omega^{\otimes k}$, from its q-expansion we can find that $\phi(f) \equiv \frac{f^p}{E_{p-1}^k}$ from which $\phi(f)$ is an invertible section if and only if f is.

We now would like to know which representation of $\pi_1^{\text{ét}}(\bar{S}_N^\zeta)$ in a $W_N(\mathbb{F}_p)$-module of rank 1 corresponds, via the equivalence in theorem 5, to the couple $(\omega^{\otimes k}, \phi)$ on $\bar{S}_N^\zeta$. It is enough to do so in the case $k = 1$. We have a favorite candidate, which is the representation of $\pi_1^{\text{ét}}(S_N^\zeta)$ on the étale quotient of the kernel of p^N on the universal elliptic curve E. Note that, if we call $\pi : E \to E^{(\phi)} = E/H$ the projection map on the canonical subgroup, the iterated $\pi_N : E \to E^{(\phi^N)}$ induces an isomorphism of the étale quotient

$$p^N E/p^n \hat{E} = p^N E/\ker(\pi^N) \xrightarrow{\sim} \ker(\check{\pi})^N \ .$$

For this to work we need the following

Lemma 1. *The representation of $\pi_1^{\acute{e}t}(S_N^\zeta)$ on $\ker(\check{\pi}^N)$ extends to a representation of $\pi_1^{\acute{e}t}(\bar{S}_N^\zeta)$, id est such representation is unramified at ∞.*

Proof. As the étale topology cannot distinguish between $\bar{S}_N^\zeta$ and $\bar{S}_1^\zeta$ is equivalent to prove that the representation of $\pi_1^{\text{ét}}(S_1^\zeta)$ on $\ker(V^N)$ extends to a representation of $\pi_1^{\text{ét}}(\bar{S}_N^\zeta)$ on $\ker(V^N)$.

Let K be the fraction field of $\bar{S}_1^\zeta$ we have to show that the inertia group of $\text{Gal}(K^{\text{sep}}/K)$ acts trivially on $\ker(V^N)$ in $E_K^{(p^N)}(K^{\text{sep}})$. We can replace K

with is completion at each cusp which is just $K((q))$ and the inverse image of E via this completion is the Tate curve $\mathrm{Tate}(q^n)/K((q))$. Following this transformation the curve E^{p^n} becomes $\mathrm{Tate}(q^{np^N})$ and $(\check{\pi})^N$ is the map

$$\mathrm{Tate}(q^{np^N}) \to \mathrm{Tate}(q^n)$$

given by the "division by the subgroup generated by q^n". As this subgroup consist only of rational points the inertia group (and also the decomposition group) acts trivially on each cusp.

□

Theorem 7. *The representation ρ of $\pi_1^{\acute{e}t}(\bar{S}_N^\zeta)$ on $\ker(\check{\pi})^N$ (which is isomorphic to the quotient of $\ker(p^N)$ on the universal curve) corresponds, via the equivalence in theorem 5, to the couple (ω, ϕ).*

Proof. It suffices to show this over S_N^ζ. Let T be a finite étale cover of S_N which trivializes the representation (we adjoin the coordinates of a point of $\ker(\check{\pi})^N$ of order exactly p^N). Over T each point of $\ker(\check{\pi})^N$ gives a morphism

$$(\mathbb{Z}/p^N\mathbb{Z})_T \xrightarrow{\sim} (\ker(\check{\pi})^N)$$

Whose Cartier dual is a morphism (note that $\ker p^N$ is in $\hat{E}$)

$$(\ker(\pi^N))_T \to (\mu_{p^N})_T \hookrightarrow (\mathbb{G}_m)_T.$$

The inverse image of the invariant differential $\frac{dt}{t}$ on $(\mathbb{G}_m)_T$ gives an invariant differential on $\ker(p^N)$ in $\hat{E}$. As T is killed by p^N, the first neighborhood of the identity section of E lies in $\ker(p^N)$ in $\hat{E}$ there is a unique invariant differential of E whose restriction to $\ker(p^N)$ in $\hat{E}$ is the given one. Thus we have

$$(\ker(\check{\pi}))_T^N \to \omega_T \ .$$

Moreover, if x is a point of $(\ker(\check{\pi}))_T^N$ of order precisely p^N the map

$$(\mathbb{Z}/p^N\mathbb{Z})_T \to (\ker(\check{\pi}))_T^N$$

is an isomorphism, and therefore its Cartier dual is an isomorphism too, meaning that the inverse image of $\frac{dt}{t}$ is nowhere vanishing on $\hat{E}$.

Thus the induced map

$$(\ker(\check{\pi})^N)_T \otimes_{\mathbb{Z}/p^N\mathbb{Z}} \mathcal{O}_T \to \omega_T$$

is an isomorphism of invertible sheaves on T. This map commutes with the action of $\mathrm{Aut}(T/S_N)$ which is defined as follows (at least locally on S, where we can assume $(\ker(p^N))_T$ in $\hat{E}$ to have coordinate ring free on the coordinates $1, x, \ldots, x^{p^N-1}$). A point P of $\ker((\check{\pi})^N)_T$ gives us a map on μ_{p^N} defined by $f(x) = \sum a_i(P)x^i$ which corresponding differential is $\omega_p = \frac{df}{f}$, and for any $g \in \mathrm{Aut}(T/S_N)$ we have $a_i(g(P)) = g(a_i(P))$.

Thus the sheaf above is $\mathrm{Aut}(T/S_N)$-equivariant and therefore it descends to S_N. Thus we have constructed an isomorphism between ω and the invertible sheaf on S_N^ζ associated to the étale quotient of ${}_{p^N}E$.

It remains to show that this isomoprhism commutes with the ϕ-linear endomorphism. Tensoring one with the inverse of the other we obtain a ϕ-linear endomorphism of $\mathcal{O}_{S_N}$ and we have now to show that it respects the identity (in other words, that carries 1 to 1).

In order to see this it suffices to show it on a"punctured disc at ∞" over $W_N(\mathbb{F}_q)((q))$ when we look at the Tate curve $\mathrm{Tate}(q^n)$. The morphism

$$\check{\pi} : \mathrm{Tate}(q^{np^N}) \to \mathrm{Tate}(q^n)$$

has kernel generated by q^n, which is a rational point of $\ker(\check{\pi})^N$, and the corresponding differential is the canonical differential on the Tate curve $\omega_{\mathrm{can}} = \frac{dt}{t}$. As q^n is a rational point, the section $[q^n] \otimes 1$ of $\ker(\check{\pi})^N \otimes_{\mathbb{Z}/p^N\mathbb{Z}} \mathcal{O}$ is fixed by the canonical F and the corresponding section ω_{can} of ω is fixed by ϕ (as it q-expansion is "identically 1"). Hence our isomoprhism respects the ϕ-linear endomorpshim on a punctured disc around ∞ implying that it respects it everywhere and we are done.

□

In order to begin to "round things up" we still need some results, namely the following theorems (due to Igusa)

Theorem 8. *The morphism*

$$\pi_1^{\acute{e}t}(\bar{S}_N^\zeta) \to \mathrm{Aut}(\ker(\check{\pi})_T^N) \cong (\mathbb{Z}/p^N\mathbb{Z})^\star$$

is surjective, and for any non-void open subset $U \subset \bar{S}_N^\zeta$ the morphism obtained by the precomposition with the map $\pi_1^{\acute{e}t}(U) \to \pi_1^{\acute{e}t}(\bar{S}_N^\zeta)$ is still surjective.

Proof. Is enough to prove that, if we denote with K the fraction field of $S_N^\zeta \times_{W_N(\mathbb{F}_q)} \mathbb{F}_q$, the morphism

$$\mathrm{Gal}(K^{sep}/K) \to \mathrm{Aut}(\ker(V^N) \text{ in } E^{(p^N)}(K^{sep}))$$

is surjective.

We will actually prove that the inertia group of $\mathrm{Gal}(K^{sep}/K)$ at any supersingular curve maps surjectively.

Let P be a closed point of S_1^ζ where E_{p-1} vanishes, by replacing $\mathbb{F}_q$ with is algebraic closure we may assume that P is rational. The completion of $S_1^\zeta \otimes \bar{\mathbb{F}}_q$ at P is isomorphic to $\mathrm{Spec}(\bar{\mathbb{F}}_q[[A]])$ and the inverse image of the universal elliptic curve on $\bar{\mathbb{F}}_q[[A]]$ admits a nowhere vanishing invariant differential ξ such that $E_{p-1}(E, \xi) = A$ as the Hasse invariants admits only simple zero (as seen in section 2).

Now we have just to prove the following

Theorem 9. *Let (E, ξ) be an elliptic curve on $\bar{\mathbb{F}}_q[[A]]$ with Hasse invariant A. Then the extension of $\bar{\mathbb{F}}_q((A))$ obtained by adding the points of $\ker V^N$ is totally ramified of degree $p^{N-1}(p-1)$ with Galois group canonically isomorphic to $\mathrm{Aut}(\mathbb{Z}/p^N\mathbb{Z})$.*

Proof. As $\ker V^N$ is cyclic of order p^N over $\bar{\mathbb{F}}_q^{sep}$ the first claim implies the second. In terms of a normalized parameter x for the formal group (meaning that $[\zeta](x) = \zeta x$ for any $p-1$-th roots of unity $\zeta \in \mathbb{Z}_p^\star$) the endomorphism $[p]$ look like

$$[p](x) = V(x^p) = Ax^p + \alpha x^{p^2} + \dots$$

for some $\alpha \in \bar{\mathbb{F}}_p[[A]]^\star$ (note that modulo A we must have, by hypothesis a supersingular curve, and therefore a formal group of height 2). Thus, as the map V^N given by the composition

$$E^{(p^N)} \xrightarrow{V^{(p^{N-1})}} E^{(p^{N-1})} \xrightarrow{V^{(p^{N-2})}} \dots \xrightarrow{V^{(p)}} E^{(p)} \xrightarrow{V} E,$$

we can look at the expression of $V^{(p^\nu)}$, which is

$$V^{(p^\nu)}(x) = A^{p^\nu} x + \alpha^{p^\nu} x^p + \dots \ .$$

A point of $\ker V^N$ with values in $K((A))^{sep}$ of order precisely p^N can be now seen as a sequence $y_0, \dots, y_{N-1}$ of elements of the maximal ideal of $\bar{\mathbb{F}}_p((A))^{sep}$ which satisfy the successive equations:

$$\begin{cases} 0 = V(y_0) = A_{y_0} + \alpha(y_0)^p + \dots \\ y_0 = V^{(p)}(y_1) = A^p y_1 + \alpha^p (y_1)^p + \dots \\ \vdots \\ y_{N-2} = V^{(p^{N-1})}(y_{N-1}) = A^{p^{N-1}} y_{N-1} + \alpha^{p^{N-1}}(y_{N-1})^p + \dots \ . \end{cases}$$

If we look at the Newton's polygons of those equation we notice that the orders of $y_0, \dots, y_{N-1}$ are given by the following (we denote with ord the normalized order such that $\mathrm{ord}(A) = 1$)

$$\begin{cases} \mathrm{ord}(y_0) = \frac{1}{p-1} \\ \mathrm{ord}(y_1) = \frac{1}{p(p-1)} \\ \vdots \\ \mathrm{ord}(y_{N-1}) = \frac{1}{p^{N-1}(p-1)} \end{cases}$$

□

□

Proposition 2. *Let k be an integer, and $N \geq 1$, then the following are equivalent:*

1. *$k \equiv 0$ modulo $(p-1)p^{N-1}$ for a prime $p \neq 2$;*

2. *the k-th tensorial power of $\pi_1^{\acute{e}t}(\bar{S}_N^\zeta)$ on the étale quotient of ${}_{p^N}E$ is trivial;*

3. *the sheaf $\omega^{\otimes k}$ on $\bar{S}_N^\zeta$ admits a nowhere vanishing F-fixed section;*

4. *it exists a nonempty open U of $\bar{S}_N^\zeta$ on which $\omega^{\otimes k}$ admits a nowhere vanishing F-fixed section;*

5. *over $\bar{S}_N^\zeta$, $\omega^{\otimes k}$ admits a section which q-expansion at one of the cusps of $\bar{S}_N^\zeta$ is identically 1;*

6. *it exists a nonempty open U of $\bar{S}_N^\zeta$ containing one cusp on which $\omega^{\otimes k}$ admits a section which q-expansion is identically 1.*

Moreover, if 1 holds, any section satisfying either 4 or 6 extends uniquely to a section on the whole $\bar{S}_N^\zeta$ satisfying respectively 3 or 5, and such section is actually the $\frac{k}{p-1}$-th power of E_{p-1}

Proof. As we have showed $\pi_1^{\text{ét}}(\bar{S}_N^\zeta)$ surjects onto $(\mathbb{Z}/p^N\mathbb{Z})^\star$ and therefore is a group of exponent $p^{N-1}(p-1)$ and hence 1 is equivalent to 2. The equivalence between 2 and 3 is a direct consequence of Theorem 7 and the one between 3 and 4 is exactly the remark we have made about the restriction being full and faithful. Using the explicit formula for ϕ and the q-expansion principle one immediately gets the equivalences between 3 and 5, and 4 and 6.

If 1 holds the statement about uniqueness comes from restriction to U being a full and faithful operation while the fact that the form is $(E_{p-1})^{\frac{k}{p-1}}$ comes from the q-expansion principle. □

Corollary 4. Let f_i for $i = 1, 2$ elements of $M(W(\mathbb{F}_q), n, k_i)$ such that $k_1 \geq k_2$, assume that the q-expansions f_1 and f_2 are congruent modulo p^N at at least one cusp of $\bar{M}(W(\mathbb{F}_q), 1)$ and that $f_1(q) \neq 0$ modulo p on such cusp. Then $k_1 \equiv k_2$ modulo $p^{N-1}(p-1)$ and if such holds on at least one cusp in each irreducible components of $\bar{M}(W(\mathbb{F}_q), 1)$, then

$$f_1 \equiv f_2(E_{p-1})^{\frac{k_1-k_2}{p-1}} \text{ modulo } p^N M(W(\mathbb{F}_q, n, k_2)).$$

Proof. It suffices tho show the congruence between the weights, as everything else follows from the q-expansion principle. If we reduce the problem modulo p^N we have, by hypothesis, that each f_i is a section of $\omega^{\otimes k_i}$ on $\bar{S}_N^\zeta$, both invertible on a non-void open subset U of $\bar{S}_N^\zeta$, therefore the quotient $\frac{f_2}{f_1}$ is an invertible section of $\omega^{\otimes(k_2-k_1)}$ on U, whose q-expansion is identically 1 on the cusps of $\bar{S}_N^\zeta$, by the proposition we have that $k_2 - k_1 \equiv 0$ modulo $p^N(p-1)$.

□

Corollary 5. Let f be a "true" modular form of level n and weight k for $\Gamma_0(p)$, holomorphic at the unramified cusps and defined on the fraction field K of $W(\mathbb{F}_q)$. Assume that at each unramified cusp the q-expansion of f has all its non-constant coefficients in $W(\mathbb{F}_q)$. Then the constant term of the q-expansion lies in $p^{-m}W(\mathbb{F}_q)$ where m is the biggest integer such that $\varphi(p^m) = \#(\mathbb{Z}/p^m\mathbb{Z})$ divides k.

Proof. For N large enough, $p^N f$ is a "true" modular form of level n and weight k for $\Gamma_0(p)$ defined on $W(\mathbb{F}_q)$. Therefore it exists a $g \in M(W(\mathbb{F}_q), n, k)$ whose q-expansions are the one of $p^N f$ at the unramified cusp. If we denote with $-m_0$ the minimal order of the constant term of those q-expansion, then g is divisible by p^{N-m_0} in $M(W(\mathbb{F}_q), n, k)$. Thus $g = p^{N-m_0} h$ for some $h \in M(W(\mathbb{F}_q), n, k)$ which hat the same q-expansion of $p^{m_0} f$ at the corresponding unramified cusps. Therefore the q-expansions of h are integral and at least one of them is congruent to a unit of $W(\mathbb{F}_q)$ modulo p^{m_0} (by minimality). Multiplying f by the inverse of such unit we have a modular form with q-expansion congruent to 1 modulo p^N. By the weight of 1 being 0 we immediately get $k \equiv 0$ modulo $p^{m_0}(p-1)$. □

4.1 Modular forms of weight χ

Let $\chi \in \mathrm{End}(\mathbb{Z}_p^\star)$, then, for each power p^N of p, χ induces an endomorphism of $(\mathbb{Z}/p^m\mathbb{Z})^\star$. For each n-th primitive root of unity ζ_n, and for each representation ρ of $\pi_1^{\text{ét}}(\bar{S}_N^{\zeta_n})$ on a free $\mathbb{Z}/p^N\mathbb{Z}$-module of rank 1 we can define $\rho^\chi = \chi \circ \rho$. If we take ρ to be the representation on the étale quotient of ${}_{p^N}E$ we denote (ω^χ, ϕ) the invertible sheaf with ϕ-linear endomorphism corresponding to ρ^χ. By varying N we obtain some compatible sheaves ω^χ on $\bar{S}_N^{\zeta_n}$.

Definition 18. A (p-adic) modular form of weight χ and level n holomorphic at ∞, defined over $W(\mathbb{F}_q)$ is a compatible family of sections of the ω^χ as above.

If $\chi = k \in \mathbb{Z} \subset \mathrm{End}(\mathbb{Z}_p^\star)$ we obtain (with this new definition) the elements of $M(W(\mathbb{F}_q), n, k)$. For $p \neq 2$ $\mathbb{Z}$ is dense in $\mathrm{End}(\mathbb{Z}_p^\star)$ and one can describe the endomorphisms as $\mathrm{End}(\mathbb{Z}_p^\star) = \varprojlim \mathbb{Z}/\varphi(p^m)\mathbb{Z}$. Thus, for each χ, the couple (ω^χ, ϕ) is isomorphic to (ω^{k_N}, ϕ) on $\bar{S}_N^\zeta$ for each $k_N \equiv \chi$ modulo $\varphi(p^N)$. Moreover, for what we have said, the isomorphism between two couples (ω^{k_N}, ϕ), $(\omega^{k'_N}, \phi)$, where $k'_N \geq k_N$ is given by multiplication by $(E_{p-1})^{\frac{k'_N - k_N}{p-1}}$. As this isomorphism doesn't actually affect the q-expansions modulo p^N, we have that a p-adic modular form of weight χ and level n, holomorphic at ∞ with coefficients in $W(\mathbb{F}_q)$, has q-expansion defined in $W[[q]]$ at each cusp, and for a given χ, f is uniquely determined by its q-expansion.

Theorem 10. *Let $\chi \in \mathrm{End}(\mathbb{Z}_p^\star)$, f a modular form of weight χ, level n, holomorphic at ∞ and defined over $W(\mathbb{F}_q)$. Then it exists a sequence of integers $0 \leq k_1 \leq k_2 \leq \ldots$ which satisfies $k_N \equiv \chi$ modulo $\phi(p^N)$ and a corresponding sequence of modular forms f_i, where f_i has weight k_i, holomorphic at ∞, defined over $W(\mathbb{F}_q)$ such that $f_N \equiv f$ in q-expansion modulo p^N.*

Conversely, let $\{k_N\}_{N \geq 1}$ a sequence of integers and suppose we have a sequence $\{f_N\}$, where $f_N \in M(W(\mathbb{F}_q), n, k_N)$ are p-adic modular forms of integer weight k_N for each N, such that $f_N \equiv f_{N+1}$ modulo p^N in q-expansion at each cusp. Then $k_N \to \chi$ in $\mathrm{End}(\mathbb{Z}_p^\star)$ and it exists a unique modular form $f =$ "$\lim$"$\{f_N\}$ of weight χ, level n holomorphic at ∞, defined over $W(\mathbb{F}_q)$ such that, for all integers N, $f_N \equiv f$ modulo p^m in q-expansion.

Proof. The first statement of the theorem follows directly form the definition of modular form of weight χ.

For the second part we may reduce ourselves to the case in which the f_m are true modular forms just by (eventually) multiplying f_m by $(E_{p-1})^{(p^{n-1}N_m)}$ for a suitable N_m, therefore we may assume $k_m \geq 0$ and the new modular form f'_m has the q-expansion of a true modular form (modulo p^m). Up to choosing the N_m to have them increasing sufficiently fast with m we have the claimed hypothesis reduction. Let us now consider the limit q-expansion. We may work on each irreducible component of $\bar{M}_n \otimes W(\mathbb{F}_q)$ separately. If on one component the limit q-expansion is identically 0 at a cusp, then we have shown that is 0 at each cusp.

If the limit q-expansion is non-zero, it must exists an m_0 such that the limit q-expansion is not divisible by p^{m_0+1} at each cusp. Thus, for $m > m_0$, $f_m \equiv p^{m_0} g_m$ where g_m is a true modular form with non trivial q-expansion modulo p. Hence, by replacing the original sequence by the sequence $\{f'_m\}$, where $f'_m = g_{m_0+m}$ we may then assume that each f_m has non-zero q-expansion modulo p. Thus, the congruence at the level of q-expansion $f_{m+1} \equiv f_m$ modulo p^m, implies the congruence $k_{m+1} \equiv k_m$ modulo $\varphi(p^m)$ between the weights and the congruence of forms $f_{m+1} \equiv f_m (E_{p-1})^{\frac{k_{m+1}-k_m}{p-1}}$ modulo p^m. Thus $\chi = \lim k_m$ is a character in $\mathrm{End}(\mathbb{Z}_p^\star)$ and the sequence of the f_m modulo p^m defines a compatible family of sections of ω^χ on $\bar{S}_N^\zeta$.

□

We can now finish with our last instance of the q-expansion principle

Corollary 6. If a collection of elements of $W[[q]]$ is the set of q-expansions of a p-adic modular form f of weight $\chi \in \mathrm{End}(\mathbb{Z}_p^\star)$, then both f and χ are uniquely determined.

A The étale fundamental group

In this appendix we want to clarify the construction of the étale fundamental group of a scheme, in order to do so we need to introduce the following concept

Definition 19. A couple $(\mathcal{C}, F)$ composed by a category $\mathcal{C}$ and a fundamental functor $F : \mathcal{C} \to \mathcal{S}ets$ is said to be a Galois category if

- $\mathcal{C}$ has terminal object $T_{\mathcal{C}}$ and pull-backs;
- $\mathcal{C}$ has finite coproducts;
- each arrow in $\mathcal{C}$ has epi-mono factorization and every monomorphism in $\mathcal{C}$ is a direct addend;
- $F(T_{\mathcal{C}}) = T_{F(\mathcal{C})}$ and F preserves pull-backs;
- F commutes with finite sums, sends epimorphisms to epimorpshims and commutes with the quotients by the action of finite groups of automorphisms.
- F reflects the isomorphism

Let $\mathcal{C}$ be a Galois category with fundamental functor F.

Definition 20. An automorphism of F is a natural isomorphism $F \to F$

We have a natural inclusion $\mathrm{Aut}(F) \subset \prod_{X \in \mathrm{Ob}(\mathcal{C})} S_{F(X)}$, where $S_{F(X)}$ is the symmetric group on $F(X)$ endowed with the discrete topology, using this inclusion we can rewrite $\mathrm{Aut}(F)$ as follows

$$\mathrm{Aut}(F) = \{(\sigma_X) \in \prod_{X \in \mathrm{Ob}(\mathcal{C})} S_{F(X)} | \sigma_Z F(f) = F(f)\sigma_Y \text{ for any } f : Y \to Z\} .$$

This tells us that $\mathrm{Aut}(F)$ is closed and therefore is profinite. Let X be an object in $\mathcal{C}$ then $\mathrm{Aut}(F)$ acts continuously on $F(X)$, we therefore obtain a structure of $\mathrm{Aut}(F)$-set $H(X)$ on $F(X)$. for $f \in \hom_{\mathcal{C}}(Y, Z)$ $F(f)$ is an $\mathrm{Aut}(F)$-morphism, hence we can define a functor $H : \mathcal{C} \to \mathrm{Aut}(F)$-$\mathcal{S}ets$ such that $F = U \circ H$ where U is the forgetful functor.

Fact 8. [5]
One has that

- H is an equivalence of categories.
- If π is a profinite group and there is an equivalence of categories π-$\mathcal{S}ets \cong \mathcal{C}$ such that $U \circ \pi \cong F$ then there is a canonic isomorphism $\pi \cong \mathrm{Aut}(F)$.
- If F' is another fundamental functor on $\mathcal{C}$ $F' \cong F$

- If π is a profinite group such that $\mathcal{C} \cong \pi\text{-}\mathcal{S}ets$ we have that $\pi \cong \mathrm{Aut}(F)$ up to an element of $\mathrm{Inn}(\mathrm{Aut}(F))$.

We want to look at the category $\mathcal{FE}t_X$ of finite étale covers of a fixed scheme X. We note that clearly 1_X is the terminal object and the fibered product of étale coverings is still an étale covering, proving that our category has pull-backs. As finite disjoint union of étale coverings is still an étale covering we have that $\mathcal{FE}t_X$ has finite coproducts. To see that our category has epi-mono factorization take $f : Y \to Z$ a morphism of coverings, we can factorize f as an epimorphism on a cover Z_1 followed by a monomorphism $\mathbb{Z}_1 \hookrightarrow Z$ where we set $\mathbb{Z} = Z_1 \sqcup Z_0$ and define $Z_0 := \{z \in Z | [Y : Z](z) = 0\}$. We will not prove (and leave it as a fact) that $\mathcal{FE}t_X$ is closed for finite quotients.

In order to define a fundamental functor on $\mathcal{FE}t_X$ we start with a algebrically closed field Ω, we then have the functor $\tilde{J} : {}_\Omega\mathcal{SA}lg \to \mathcal{S}ets$ defined by taking the set of morpshisms $B \mapsto \mathrm{Hom}_\Omega(B, \Omega)$, so that we immediately get the functor $J : \mathcal{FE}t_{\mathrm{Spec}(\Omega)} \to \mathcal{S}ets$. We now can take the base-change induced functor $\mathcal{FE}t_X \to \mathcal{FE}t_{\mathrm{Spec}(\Omega)}$ and set F to be the composite.

Definition 21. With the notation above we call étale fundamental group of a scheme X the group $\pi^{\text{ét}}(X) := \mathrm{Aut}(F)$.

In order to give an easier way to look at the fundamental group we have to introduce the concept of a Galois object.

Definition 22. Let A be a finite étale cover of X, we say that A is Galois if $A/\mathrm{Aut}(A) \cong 1_X$, which is equivalent to ask that the action of $\mathrm{Aut}(A)$ is transitive (and therefore that $\#\mathrm{Aut}(A) \geq \#F(A)$).

One can actually show $\mathrm{Hom}(A, B) \hookrightarrow F(B)$ from which we get that, if A is Galois $\#F(A) = \#\mathrm{Aut}(A)$. We will now build a couple (A, a) composed by a Galois covering A such that $\mathrm{Hom}_{\mathcal{C}}(A, X) \to F(X)$ is a bijection and an element $a \in F(A)$. To do so start with $Y = B^{F(B)} = \prod_{F(B)} B$ and let $a \in F(Y) = F(B)^{F(B)}$ such that the b-th coordinate is b for $b \in F(B)$ and let A the connected component of Y for which $a \in F(A)$, then we have

$$A \longrightarrow Y \xrightarrow{p_b} B$$

from which $\mathrm{Hom}(A, B) \to F(B)$ is surjective (one can show that A is Galois by using the point a to keep track of the connected component we are considering, to see this one can refer to [5, pp 40-41]).

From this we can build $\pi_1^{\text{ét}}(Z)$ by setting $J = \{(A, a)\}$ as above, then J is cofinite in $\mathcal{FE}t_X$. As $F \cong \mathrm{Hom}_{\mathcal{FE}}\, t_X(A, -)$. If $(A, a) \geq (B, b)$ we have, for all σ

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\tau} \\ A & \xrightarrow[f]{} & B \end{array}$$

From which $F(\tau)(b) = F(f\sigma)(a)$ form which $\sigma \mapsto \tau$ defines a projective system and we have

$$\pi = \lim_{\leftarrow J} \mathrm{Aut}(A).$$

B The "Lang's trick"

In order to get the equivalence in Theorem 5 we use that a finite dimensional vector space over an algebraically closed field K endowed with a q-linear automorphism ϕ is generated by the fixed points of ϕ.

Proposition 3. *Let ϕ be a q-linear endomorphism of a finite dimensional vector space V over a separably closed field K of positive characteristic.*

Call $V^{1-\phi} = \ker(1-\phi)$ the $\mathbb{F}_q$ vector space of fixed points of ϕ, then one has

$$V \cong V^{1-\phi} \otimes_{\mathbb{F}_q} K \ .$$

Proof. Let e be a K-basis of V and write

$$\phi(e) = Ae$$

for some $A \in \mathrm{GL}(n, K)$. Call

$$F : \mathrm{GL}(n, k) \to \mathrm{GL}(n, k)$$

the map given by "elevating coordinates at the q-th power". Then, for $g \in \mathrm{GL}(n, k)$, ge is a basis of V of ϕ-fixed points if and only if we have

$$F(g)Ag^{-1} = 1 \ .$$

Call $\bar{K}$ the algebraic closure of K. We define an action of the group $\mathrm{GL}(n, \bar{K})$ on itself (seen as an algebraic variety) by setting

$$gA = F(g)Ag^{-1} \ .$$

For each fixed A the map $g \mapsto F(g)Ag^{-1}$ is étale (one can see this just by computing the tangent map) and hence the orbits of our action must be open. As $\mathrm{GL}(n, \bar{K})$ is irreducible it must have only one orbit, which means nothing more that the map $g \mapsto F(g)g^{-1}$ is surjective. As this is étale too and K is separably closed the restriction to $\mathrm{GL}(n, K)$ must be surjetcive as well, meaning that V admits a basis of ϕ-fixed points. It is now clear (by q-linearity of ϕ) that all ϕ-fixed points are in the $\mathbb{F}_q$-vector space generated by a basis of ϕ-fixed points of V, which proves the statement.

□

C Newton Polygons

Let $f(x) = 1 + a_1 x + \dots a_s x^s$ be a polynomial $\hat{\bar{\mathbb{Q}}}_p[x]$, and consider the set of points of $\mathbb{R}^2$ given by $P = \{(n, \mathrm{ord}_p(a_n))\}_{1 \leq n \leq s} \cup (0,0)$ for $a_i \neq 0$ (in such case we can think of the point as if it was "infinitely" far above the horizontal axis).

Definition 23. The Newton polygon of f is the convex hull of the set P, id est the highest convex polygonal line such that any point in P lies either on the polygonal line or above it.

To construct such polygon one simply start from the origin and draws the line passing from $(0,0)$ and the point α_1 in P which is the first we encounter by moving counter-clockwise on the sheaf of lines through $(0,0)$, if such line hits more than one point at the same time we take the furthest one. Then we repeat this process centering the lines in $\alpha_1 = (n_1, \mathrm{ord}_p(a_{n_1}))$, considering now $P_1 = \{\alpha = (n, \mathrm{ord}_p(a_n)) \in P | n > n_1\}$ and so on. As the coefficients of the polynomial are finite this process ends and we get the desired polygon.

Definition 24. We call vertexes of a Newton polygon the points in P that lies on the polygon, we refer to slope of the segment joining to vertexes as the slope of the segment in the usual way and we call length of a slope the distance on the horizontal axis of the points it connects

The reason to study those arises from the following

Lemma 2. *Let $f \in \hat{\bar{\mathbb{Q}}}_p[x] = \prod_{i=1}^{s} (1 - \frac{x}{b_k})$. Let $\lambda_k = ord_p(\frac{1}{b_k})$, then if λ is a slope of the newton polygon of f of length l, exactly l of the λ_k are equal to λ*

Meaning that the slopes of the newton polygons are exactly (counting multiplicity) the p-adic ordinals of the reciprocal roots of f.

Proof. We may assume $\lambda_1 \leq \dots \leq \lambda_s$, furthermore we may assume that the first r of the λ_k are the same and strictly less than λ_{r+1} for some $1 \leq r \leq s$.

We claim that the first segment of the Newton polynomial associated to f connects $(0,0)$ to $(r, r\lambda_1)$. Recall that a_i can be expressed as $(-1)^i$ times the evaluation of the i-th symmetric polynomial in s variables at the $\frac{1}{b_k}$. Therefore the ordinal of such is at least $i\lambda_1$, therefore the point $(i, \mathrm{ord}_p(a_i))$ is either above or lies on the line $(i, i\lambda_1)$, proving this first claim.

Consider now a_r. There is exactly one product of r of the $\frac{1}{b_k}$ having valuation exactly $r\lambda_1$, namely the product of the first r, while all others have strictly bigger ordinals. Thus, a_r is the sum of something of ordinal $r\lambda_1$ and something having strictly bigger ordinal. Hence $\mathrm{ord}_p(a_r) = r\lambda_1$. As $\mathrm{ord}_p(a_r + 1) > r\lambda$ inducing this argument we get the thesis.

□

Although this result is quite powerful, it is not enough for what we want to do in section 4, as we are dealing with some formal groups and therefore with power series, therefore we need to introduce an analogous concept for those objects.

Definition 25. Let $f = 1 + a_1x + a_2x^2 + \cdots \in \hat{\bar{\mathbb{Q}}}_p[[x]]$ be a power series with constant term 1 and non-0 radius of convergence. Let $f_n = 1 + \sum_{i=1}^{n} a_i x^i$, then we define the Newton polygon of f as the limit of the Newton polygon of the f_n.

Although this definition might seem difficult the way to construct this remains the same (at least "algorithmically" if you want). The issue and that having to deal with an infinite set of points reflects in the possibility of few pathological behaviors. This time our "output" can be one of the following:

1. An infinite number of segments of finite length (e.g $f(x) = 1 + \sum p^{i^2} x^i$)
2. A polygonal line that ends with a half-line, meaning that our procedure hits simultaneously a set of points which lie arbitrarily far out. (e.g. $f(x) = 1 + \sum x^i$)
3. The strangest possibility happens when we pass from a situation in which we have not yet encountered any point to extend our polygon to a configuration in which our line would be above some of the points we still have not hit, in this case we prolong our polygon with slope equal to the upper bound of the slopes such that no point is beneath them (e.g. $f(x) = 1 + \sum px^i$)

Note that the third case can degenerate if the first step is the one when this behavior appears, in such a case one can prove that f has radius of convergence 0, so we avoid this problem just by requiring a non-trivial radius of convergence.

We now have two results (before to get to what we really care about) that we will only quote. For a proof of those see [4, pp 101-103].

Lemma 3. *Let B be the least upper bound of all slopes of the Newton polygon of $f(x)$. Then the radius of convergence of $f(x)$ is p^B (if B is infinite f converges on the whole space).*

Lemma 4. *Suppose that λ_1 is the first slope of the Newton polygon of $f(x)$. Let $c \in \hat{\bar{\mathbb{Q}}}_p$ be of ordinal $\lambda \leq \lambda_1$. Suppose that $f(x)$ converges in $D(p^\lambda)$ (Note that by the previous lemma this holds automatically if the inequality above is strict).*

Let now

$$g(x) = (1 - cx)f(x) \ .$$

Then the Newton polygon of $g(x)$ is obtained by connecting $(0, 0)$ to $(1, \lambda)$ and then translating the newton polygon of $f(x)$ by 1 to the right and by λ upwards. To picture this, just imagine to glue the Newton polygon of $f(x)$ to the new segment (which is the Newton polygon of $1 - cx$). Moreover if $f(x)$ has last slope λ_f, then f converges in $D(p^{\lambda_f})$ if and only if $g(x)$ does.

We end this appendix with the result we are interested in, namely the following

Lemma 5. *Let $f(x) \in 1+x\hat{\bar{\mathbb{Q}}}_p$ have Newton polygon with first slope λ_1. Suppose that $f(x)$ converges on the closed disc $D(p^{\lambda_1})$, and assume also that the line through $(0,0)$ with slope λ_1 passes through a point of the form $(i, ord_p(a_i))$ (Note that both of those hold if the polygon has more than one slope). Then it exists a t such that $ord_p(t) = -\lambda_1$ and $f(t) = 0$*

Proof. We start by proving the case in which $\lambda_1 = 0$. In such case we have $\mathrm{ord}_p(a_i) \geq 0$ for all i and the sequence of the $\mathrm{ord}_p(a_i) \to \infty$ when we let i diverge. Let N be the greatest i such that $\mathrm{ord}_p(a_i) = 0$ (if the polygon is not just a horizontal line this N is the length of the first segment of slope $\lambda_i = 0$).

Let now $f_n(x) = \sum_{i=1}^{n} a_i x^i$. By Lemma 2, for $n \geq N$ $f_n(x)$ has exactly N roots $t_{n,1}, \ldots, t_{n,N}$ such that $\mathrm{ord}_p(t_{n,j}) = 0$. Set $t_N = t_{N,1}$ and for $n \geq N$ call t_{n+1} any of the $t_{n+1,j}$ such that $|t_{n+1,j} - t_n|_p$ is minimal. We claim that the sequence $\{t_n\}$ is Cauchy and that, calling $t = \lim_{n\to\infty} t_n$ has the desired properties.

For $n \geq N$ call S_n the set of roots of $f_n(x)$ (counting multiplicity). Then for $n \geq N$ one has

$$|f_{n+1}(t_n) - f_n(t_n)|_p = |f_{n+1}(t_n)|_p = \prod_{t\in S_n} |1 - \frac{t_n}{t}|_p =$$

$$\prod_{i=1}^{n} |1 - \frac{t_n}{t_{n+1,i}}|_p = \prod_{i=1}^{N} |t_{n+1,i} - t_n|_p \geq |t_{n+1} - t_n|_p^N \ .$$

Therefore

$$|t_{n+1} - t_n|_p^N \geq |f_{n+1}(t_n) - f_n(t_n)|_p = |a_{n+1} t_n^{n+1}|_p = |a_{n+1}|_p \ .$$

And therefore the sequence $\{t_n\}$ is Cauchy as $\lim_{n\to\infty} |a_{n+1}|_p = 0$. Call now $t = \lim_{n\to\infty} t_n$, then as $f = \lim f_n$ one has

$$|f_n(t)|_p = |f_n(t) - f_n(t_n)|_p = |t - t_n|_p | \sum_{i=1}^{n} a_i \frac{t^i - t_n^i}{t - t_n}|_p \leq |t - t_n|_p$$

as we have that $|a_i|_p \leq 1$ and $|\frac{t^i - t_n^i}{t - t_n}|_p = |t^{i-1} + t^{i-2} t_n + \cdots + t t_n^{i-2} + t_n^{i-1}|_p \leq 1$. Hence $f(t) = \lim_{n\to\infty} f_n(t) = 0$, proving the statement for $\lambda_i = 0$.

For the general case, we have $\lambda_1 = \mathrm{ord}_p(\pi)$ for some $\pi \in \hat{\bar{\mathbb{Q}}}_p$. Now call $g(x) := f(\frac{x}{\pi})$, then $g(x)$ has a Newton polygon with $\lambda_1 = 0$, so that we can apply what we have just shown, ending up with a t_0 such that $\mathrm{ord}_p(t_0) = 0$ and $g(t_0) = 0$. Call $t = \frac{t_0}{\pi}$, we have that $\mathrm{ord}_p(t) = -\lambda_1$ and $f(t) = f(\frac{t_0}{\pi}) = g(t_0) = 0$, finishing the proof.

□

References

[1] Pierre Deligne and N Katz. *Groupes de Monodromie en Geometrie Algebrique: Seminaire de Geometrie Algebrique du Bois-Marie 1967-1969 (SGA 7 II)*, volume 340. Springer, 2006.

[2] Fred Diamond and Jerry Michael Shurman. *A first course in modular forms*, volume 228. Springer, 2005.

[3] Nicholas M Katz. P-adic properties of modular schemes and modular forms. In *Modular functions of one variable III*, pages 69–190. Springer, 1973.

[4] Neal Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, volume 58. Springer Science & Business Media, 2012.

[5] Henrik W Lenstra. Galois theory for schemes.

[6] Jean-Pierre Serre. Formes modulaires et fonctions zêta p-adiques. In *Modular functions of one variable III*, pages 191–268. Springer, 1973.

[7] Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer Science & Business Media, 2009.

[8] Henry Peter Francis Swinnerton-Dyer. On ℓ-adic representations and congruences for coefficients of modular forms. In *Modular functions of one variable III*, pages 1–55. Springer, 1973.