p-adic Modular Forms à la Serre

Samuel Marks

5 February, 2020

1 Introduction

These notes are for a lecture given at STAGE. They cover the basics of Serre's theory of p-adic modular forms, as presented in [2]. In this concrete and elementary theory, Serre defines a p-adic modular form (on $\mathrm{SL}_2(\mathbb{Z})$) to be a q-expansion $f \in \mathbb{Q}_p[\![q]\!]$ which is the p-adic limit of q-expansions of classical modular forms. Theorems are proved about p-adic modular forms by studying the algebra $M(\mathbb{F}_p)$ of mod p modular forms, which is nothing more than the collection of q-expansions $f \in \mathbb{F}_p[\![q]\!]$ that are mod p reductions of classical modular forms. Especially important is a result of Swinnerton-Dyer which shows that the kernel of this reduction map is generated by $E_{p-1} - 1$, where E_{p-1} is an Eisenstein series.

Despite its elementarity, Serre's theory proves fruitful. Here we present the two applications that most motivated Serre's work: proving congruence properties of modular forms and constructing p-adic zeta functions. Both of these applications capture the general principal that the nonconstant Fourier coefficients of a p-adic modular form determine the constant term. Moreover, by studying how the nonconstant terms of Eisenstein series vary in a family, Serre easily deduces that the p-adic zeta function is *continuous*.

Nowadays, the study of p-adic modular forms finds its foundations in Katz's geometric appraoch (see [1]) instead of Serre's theory. Accordingly, STAGE will study Katz's theory in greater detail. Why, then, are we spending a lesson on Serre's theory? I think there are three reasons. First, the concreteness of Serre's theory helps to fix ideas. We will encounter many objects – such as the ordinary space, the ordinary projector, the p-adic weight space, and the space of p-adic or mod p modular forms themselves – which will reappear in Katz's framework with much more abstract definitions. Serre's theory provides concrete models of these objects, making them much easier to think about. Second, and relatedly, the simplicity of the theory makes clear what sort of problems we hope to solve with the study of p-adic modular forms, and what sorts of methods will be useful. And third, Serre's theory gives us great results with minimal set-up; questions posed at the start of the lecture will be answered by the end, not after wading through three lectures of complicated algebraic geometry. We simply can't resist the instant gratification.

Throughout p denotes a prime. Although results are stated in general, we will restrict proofs to the case $p \geq 3$ or $p \geq 5$ when simpler. Following Serre, we will also consider modular forms on the full modular group $\mathrm{SL}_2(\mathbb{Z})$ only. The space of weight k classical modular forms is denoted M_k.

2 Motivation

We explain here some of the things on Serre's mind that led him to formulate a p-adic theory of modular forms. We'll also fix some notation that will be used in the rest of the notes.

2.1 Modular forms congruences

Let $j = \frac{E_4^3}{\Delta}$ be the modular j function, normalized so that

$$j = q^{-1} + 744 + 196884q + \cdots = 744 + \sum_{n \geq -1} c(n)q^n$$

for integers $c(n) \in \mathbb{Z}$. In 1949, Lehner proved some interesting divisibility properties of these integers mod $p = 2, 3, 5, 7$.

Theorem 1 (Lehner)**.** *For all natural numbers $\alpha \geq 1$,*

$$\begin{aligned} c(2^\alpha n) &\equiv 0 \pmod{2^{3\alpha+8}} \\ c(3^\alpha n) &\equiv 0 \pmod{3^{2\alpha+3}} \\ c(5^\alpha n) &\equiv 0 \pmod{5^\alpha + 1} \\ c(7^\alpha n) &\equiv 0 \pmod{7^\alpha}. \end{aligned}$$

There is also a similar congruence for $p = 11$. Lehner proved these congruences via esplicit prime-by-prime computation, leaving something to be desired conceptually.

To view these congruences differently, let U_p be a linear operator which acts on a q-expansion $\sum a(n)q^n$ via

$$\left(\sum a(n)q^n\right) | U_p = \sum a(pn)q^n.$$

Then the theorem implies that $(j - 744)|U_p^n \to 0$ in the p-adic limit. We will see how Serre's theory gives an easy, conceptual proof of theorems of this sort.

2.2 p-adic L-functions

Recall that the values of $\zeta(s)$ at negative odd integers are

$$\zeta(1 - k) = -\frac{B_k}{k}$$

where B_k is the kth Bernoulli number. Bernoulli numbers have some interesting divisibility properties. Here is an easy theorem about Bernoulli numbers.

Theorem 2 (Clausen-von Staudt)**.** *For all $k \in \mathbb{N}$, we have*

$$B_k + \sum_{\substack{p \text{ prime} \\ p-1|k}} \frac{1}{p} \in \mathbb{Z}.$$

In particular, $v_p(B_k) = -1$ if $(p-1)|k$, and $v_p(B_k) \geq 0$ otherwise.

And here's a harder theorem about Bernoulli numbers.

Theorem 3 (Kummer congruences)**.** *If $k, k' \in \mathbb{N}$ are even with $k \equiv k' \not\equiv 0 \pmod{p-1}$ then*

$$\frac{B_k}{k} \equiv \frac{B_{k'}}{k'} \mod p.$$

More generally, if $k, k' \in \mathbb{N}$ are even, not divisible by $p - 1$, and $k \equiv k' \pmod{p^a(p-1)}$ then

$$(1 - p^{k-1})\frac{B_k}{k} \equiv (1 - p^{k'-1})\frac{B_{k'}}{k'} \pmod{p^{a+1}}.$$

A reader experienced with L-functions will recognize the numbers appearing in the general Kummer congruences as special values of the Riemann zeta function with its p-part stripped out. Therefore, the Kummer congruences indicate some sort of p-adic continuity properties of the function $(1-p^{-s})\zeta(s)$. Indeed, the Kummer congruences were used by Kubota and Leopoldt to construct a *p-adic L-function* that interpolated the values of ζ. We present below Serre's construction of the p-adic zeta function, which is much simplier and whose proof does *not* rely on the Kummer congruences.

3 Eisenstein series and congruences

We denote by G_k and E_k the weight k Eisenstein series, normalized so that

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

Recall that for $k > 2$ these are modular forms on $\mathrm{SL}_2(\mathbb{Z})$ and that the algebra of modular forms on $\mathrm{SL}_2(\mathbb{Z})$ is generated by E_4 and E_6. This implies, for example, that $\dim M_8 = 1$ and $E_4^2 = E_8$ since they are both weight 8 modular forms with the same constant term.

By Clausen-von Staudt's theorem, we have $v_p(k/B_k) \geq p^{a+1}$ when $k \equiv 0 \pmod{p^a(p-1)}$ so that $E_{p-1} \equiv 1 \pmod{p}$, and more generally $E_{p^a(p-1)} \equiv 1 \pmod{p^{a+1}}$. Having noted these congruences, we fix the following notation.

Definition 4.

(1) $M_k(\mathbb{Z}_{(p)}) = M_k \cap \mathbb{Z}_{(p)}[\![q]\!]$ denotes the $\mathbb{Z}_{(p)}$-module of weight k modular forms with p-integral Fourier coefficients. We denote by $M_k(\mathbb{F}_p)$ the image of the reduction mod p map $M_k(\mathbb{Z}_{(p)}) \to \mathbb{F}_p[\![q]\!]$, $f \mapsto \overline{f}$.

(2) Since $E_{p-1} \equiv 1 \pmod{p}$ we have inclusions

$$M_k(\mathbb{F}_p) \subseteq M_{k+p-1}(\mathbb{F}_p) \subseteq M_{k+2(p-1)}(\mathbb{F}_p) \subseteq \cdots$$

and for $\alpha \in \mathbb{Z}/(p-1)\mathbb{Z}$ we set

$$M^{\alpha}(\mathbb{F}_p) = \bigcup_{k\equiv\alpha \pmod{p-1}} M_k(\mathbb{F}_p).$$

(3) We set $M(\mathbb{F}_p) = \sum_k M_k(\mathbb{F}_p)$ to be the subalgebra of $\mathbb{F}_p[\![q]\!]$, and similarly for $M(\mathbb{Z}_{(p)})$.

We know that $E_{p-1} - 1$ is in the kernel of the reduction map $M(\mathbb{Z}_{(p)}) \to M(\mathbb{F}_p)$. In fact, its is the whole kernel.

Theorem 5 (Swinnerton-Dyer)**.**

(1) For $p \geq 5$ we have $M(\mathbb{F}_p) = \mathbb{F}_p[\overline{E}_4, \overline{E}_6]/(\overline{E}_{p-1} - 1)$. This $\mathbb{F}_p$-space is a direct sum

$$M(\mathbb{F}_p) = \bigoplus_{\alpha\in\mathbb{Z}/(p-1)\mathbb{Z}} M^{\alpha}(\mathbb{F}_p).$$

(2) *For $p = 2, 3$, we have $M(\mathbb{F}_p) = M^0(\mathbb{F}_p) = \mathbb{F}_p[\overline{\Delta}]$ for the weight-12 cusp form Δ.*

This structure theorem has the following crucial consequence.

Theorem 6. *Let $f, f' \in M(\mathbb{Z}_{(p)})$ be nonzero of weights k, k'. If*

$$f \equiv f' \pmod{p^m}$$

then

$$\begin{aligned} k &\equiv k' \pmod{p^{m-1}(p-1)} && \text{if } p \geq 3 \\ k &\equiv k' \pmod{2^{m-2}} && \text{if } p = 2. \end{aligned}$$

For $p \geq 5$ and $m = 1$, the theorem follows immediately from Theorem 5 since $f \equiv f' \pmod{p}$ implies that f, f' are in the same component $M^\alpha(\mathbb{F}_p)$ of $M(\mathbb{F}_p)$ so that $k \equiv k' \pmod{p-1}$. The full proof of the $m \geq 2$ case requires a deeper study of *filtrations* and is relegated to the appendix. However, we'll mention here a key ingredient of the proof.

Definition 7. The *Ramanujan theta operator* is a differential operator defined by

$$\Theta = q\frac{d}{dq}$$

so that $\Theta\left(\sum a(n)q^n\right) = \sum na(n)q^n$.

Two key properties of Θ are given here.

Proposition 8.

(1) *Θ "almost" increases the weight of a modular form by 2. More precisely, for a weight k modular form f, we have $\Theta(f) = \frac{\tilde{f}+kfE_2}{12}$ where $\tilde{f}$ is modular of weight $k+2$. (Recall that E_2 is not a modular form.)*

(2) *If $f \in M^\alpha(\mathbb{F}_p)$ then $\Theta(f) \in M^{\alpha+2}(\mathbb{F}_p)$.*

Note that (2) follows easily from (1): we have that $E_{p+1} = E_2E_{p-1} \equiv E_2 \pmod{p}$ so that fE_2 is congruent to a modular form of weight $k + p + 1$. The theta operator will reappear in the theory of Katz, defined in abstract Hodge-theoretic language.

As another consequence of Theorem 5, we can prove the Kummer congruences for $a = 1$.

Proof of Kummer congruences for $a = 1$. If $k \equiv k' \not\equiv 0 \pmod{p-1}$ then $\sigma_{k-1}(n) \equiv \sigma_{k'-1}(n) \pmod{p}$ for all n. Since $p - 1 \nmid k, k'$, Clausen-von Staudt gives $G_k, G'_k \in M(\mathbb{Z}_{(p)})$. Hence

$$M^k(\mathbb{F}_p) \ni \overline{G}_k - \overline{G}_{k'} = \frac{B_k}{k} - \frac{B_{k'}}{k'} \in M^0(\mathbb{F}_p).$$

As $k \not\equiv 0 \pmod{p-1}$, Theorem 5 asserts that this quantity is 0, so that $\frac{B_k}{k} - \frac{B_{k'}}{k'} \equiv 0 \pmod{p}$ as desired. $\square$

4 p-adic modular forms

We finally are ready to define p-adic modular forms.

Definition 9. A *p-adic modular form* is a power series $f \in \mathbb{Q}_p[\![q]\!]$ such that there is a sequence of modular forms $f_i \in M(\mathbb{Q})$ with rational coefficients with $f = \lim f_i$. In other words, the space $M(\mathbb{Q}_p)$ of p-adic modular forms is the p-adic completion of $M(\mathbb{Q})$.

Let f be a p-adic modular form, and let k_i be the weights of the $f_i \in M_{k_i}(\mathbb{Q})$ converging to f. By Theorem 6, for all $m \geq 1$, the k_i eventually becomes stationary in $\mathbb{Z}/p^m(p-1)\mathbb{Z}$. It follows that the weights have a limit $k = \lim k_i$ in

$$\mathfrak{X} = \varprojlim \mathbb{Z}/p^m(p-1)\mathbb{Z} \cong \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$$

and this limit is independent of the sequence of f_i chosen. We call k the *weight* of f, and denote by $M_k(\mathbb{Q}_p)$ the space of p-adic modular forms of weight k.

Remark 10. The significance of $\mathfrak{X} \cong \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$ is that $\mathfrak{X}$ is the space of continuous characters $\mathbb{Z}_p^\times \to \mathbb{C}_p^\times$. Indeed, since $\mathbb{Z}_p$ contains the $(p-1)$st roots of unity, all of which are incongruent mod p, the reduction map

$$0 \longrightarrow 1 + p\mathbb{Z}_p \longrightarrow \mathbb{Z}_p^\times \longrightarrow \mathbb{F}_p^\times \longrightarrow 0$$

splits, giving

$$\mathbb{Z}_p^\times = \mu_{p-1} \times (1 + p\mathbb{Z}_p).$$

The characters of $1 + p\mathbb{Z}_p$ are given by $\alpha \mapsto \alpha^k$ for $k \in \mathbb{Z}_p$. Thus, the characters of $\mu_{p-1} \times (1 + p\mathbb{Z}_p)$ are given by

$$(u, \alpha) \mapsto (u^h, \alpha^k)$$

for some $(h, k) \in \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$. This makes conceptual sense: from the example of Eisenstein series we see that weights are things used in exponents, and characters of $\mathbb{Z}_p^\times$ all come from exponentiating.

For a (p-adic) modular form $f = \sum a_n q^n$, let $v_p(f) = \inf_n v_p(a_n)$. Since any modular form can be scaled to have integral Fourier coefficients, we have $v_p(f) > -\infty$. The following is a restatement of Theorem 6.

Proposition 11.

(1) Let $f, f' \in M(\mathbb{Q})$ be nonzero with weights k, k' satisfying

$$v_p(f - f') \geq v_p(f) + m$$

for $m \geq 1$. Then

$$\begin{aligned} k &\equiv k' \pmod{(p-1)p^{m-1}} && \text{if } p \geq 3 \\ k &\equiv k' \pmod{2^{m-2}} && \text{if } p = 2. \end{aligned}$$

(2) The same is true for p-adic modular forms $f, f' \in M(\mathbb{Q}_p)$.

Proof. For part (1), we have

$$p^{-v_p(f)} f \equiv p^{-v_p(f)} f' \pmod{p^m}$$

so that $f, f' \in M(\mathbb{Z}_{(p)})$ and the result follows from Theorem 6. Part (2) follows immediately. $\square$

The thrust of the following propositions is that p-adic properties of the nonconstant Fourier coefficients give information about the constant coefficient.

Proposition 12.

(1) Let $f = \sum a_n q^n \in M_k(\mathbb{Q}_p)$ for $k \in \mathfrak{X}$. If $m \geq 0$ is such that $k \not\equiv 0 \pmod{p^m(p-1)}$ then

$$v_p(a_0) + m \geq \inf_{n \geq 1} v_p(a_n).$$

(2) Let $f^{(i)} = \sum a_n^{(i)}$ be a sequence of p-adic modular forms of weight $k^{(i)} \in \mathfrak{X}$. If

(a) the $a_n^{(i)} \overset{i \to \infty}{\longrightarrow} a_n$ uniformly in n, and

(b) the $k^{(i)} \overset{i \to \infty}{\longrightarrow} k \neq 0$

then also $a_0 \overset{i \to \infty}{\longrightarrow} a_0$, and $f = \sum_{n \geq 0} a_n q^n \in M_k(\mathbb{Q}_p)$.

Proof. (1). If $a_0 = 0$ we are done. Otherwise, since $a_0 \in M_0(\mathbb{Q}_p)$, the contrapositive of proposition 11 gives

$$\inf_{n \geq 1}(a_n) = v_p(f - a_0) < v_p(f) + m + 1.$$

Thus $v_p(a_0) + m \geq v_p(f) + m \geq \inf_{n \geq 1} v_p(a_n)$.

(2). Since $k \neq 0$, we can pick m large enough that $k \not\equiv 0 \pmod{p^m(p-1)}$. By the uniformity assumption in (a), we can pick $t \in \mathbb{Z}$ so that $v_p(a_n^{(i)}) \geq t$ for all $n \geq 1$ and $i \gg 0$. By part (1) we have $v_p(a_0^{(i)}) > t - m$ for all $i \gg 0$. As $p^{t-m}\mathbb{Z}_p$ is compact, we have that some subsequence of the $a_0^{(i)}$ has a limit a_0 and that $f = \sum_{n \geq 0} a_n q^n \in M_k(\mathbb{Q}_p)$. If a_0' is a limit of a different subsequence then $f' = a_0 + \sum_{n \geq 1} a_n q^n \in M_k(\mathbb{Q}_p)$ as well so that

$$f - f' = a_0 - a_0' \in M_k(\mathbb{Q}_p) \cap M_0(\mathbb{Q}_p) = 0.$$

Hence $a_0^{(i)}$ converges to a_0. $\square$

Note that this is a rather mild example of the p-adic properties of nonconstant coefficients giving information about the constant term. We will see more extreme examples later.

5 The p-adic zeta function

Let σ_k^* denote the kth-power divisor sum with the p-part removed:

$$\sigma_k^*(n) = \sum_{\substack{d \mid n \\ p \nmid d}} d^k.$$

Since all of the d appearing in the sum are units in $\mathbb{Z}/p^m\mathbb{Z}$ for any $m \geq 1$ we see that

$$\sigma_k^*(n) \equiv \sigma_{k'}^*(n) \pmod{p^m} \quad \text{when } k \equiv k' \pmod{p^{m-1}(p-1)}.$$

Also note that if $k_i \in \mathbb{Z}$ is a sequence of integers converging to $k \in \mathfrak{X}$ with $k_i \to \infty$ in the archemedian sense, then

$$\sigma_{k_i}(n) \to \sigma_k^*(n) \quad \text{uniformly in } n.$$

As the numbers on the left are Fourier coefficients of the Eisenstein series G_{k_i} proposition 12(2) gives the following.

Proposition 13. *For $0 \neq k \in \mathfrak{X}$ even, there is a p-adic modular form*

$$G_k^* = a_0 + \sum_{n \geq 1} \sigma_{k-1}^*(n)$$

where

$$a_0 = \lim_{i \to \infty} \frac{-B_{k_i}}{2k_i} = \frac{1}{2} \lim_{i \to \infty} \zeta(1 - k_i).$$

We denote this constant term by $\zeta^*(1-k)$. Thus $\zeta^*(k)$ defines a function on the odd $k \in \mathfrak{X} - \{1\}$; we call this the *$p$-adic zeta function*. Since the nonzero Fourier coefficients of G_k^* vary continuously with k, proposition 12(2) shows that ζ^* is *continuous*! Note that since $k_i \to \infty$ in the archemedian sense, if $k \geq 2$ is an *integer* then

$$\zeta^*(1-k) = \lim_{i \to \infty} \zeta(1 - k_i) = \lim_{i \to \infty} \prod_{\ell \text{ prime}} \frac{1}{1 - \ell^{k_i - 1}} = \prod_{\ell \neq p} \frac{1}{1 - \ell^{k_i - 1}} = (1 - p^{k-1})\zeta(1-k).$$

Remark 14. Since ζ^* is continuous and interpolates the values of $(1-p^{k-1})\zeta(1-k)$ on a p-adically dense set of integers, it must be none other than the Kubota-Leopoldt L-function! More precisely for $p \neq 2$ and $(s, u) \in \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z} \cong \mathfrak{X}$ we have

$$\zeta^*(s, u) = L_p(s, \omega^{1-u})$$

where ω is the Teichmuller character. (There is a similar statement for $p = 2$.) So Serre not only constructed L_p, he did it without using the Kummer congruences in a way that gives continuity for free!

6 More congruences

Recall the operator U_p defined by

$$\left(\sum a(n) q^n\right) | U_p = \sum a(pn) q^n.$$

In this section we will summarize results about the action of U_p on $M(\mathbb{F}_p)$. The takeaway is a decomposition $M(\mathbb{F}_p) = S \oplus N$ where U_p is bijective on S and nilpotent on N. Moreover S is finite-dimensional and easy to compute, making it easy to understand the eventual behavior of $f|U_p^n$.

Recall that for primes ℓ, Hecke operator T_ℓ acts on the Fourier expansion of a weight k modular form via

$$\left(\sum a(n) q^n\right) | T_\ell = \sum a(\ell n) q^n + \ell^{k-1} \sum a(n) q^{\ell n}$$

which is another modular form of weight k. Hence for $k \in \mathbb{N}$ we have $f|T_p \equiv f|U_p \pmod{p}$, so that U_p gives a map $M_k(\mathbb{F}_p) \to M_k(\mathbb{F}_p)$. Also, if $f \in M_k(\mathbb{Q}_p)$ with $k \in \mathfrak{X}$, then picking a sequence of $f_i \in M_{k_i}(\mathbb{Q})$ converging to f so that $k_i \to \infty$ in the archemedian sense, we see

$$f_i | T_p \to f | U_p$$

so that U_p gives a map $M_k(\mathbb{Q}_p) \to M_k(\mathbb{Q}_p)$.

Recall the inclusions

$$M_k(\mathbb{F}_p) \subseteq M_{k+p-1}(\mathbb{F}_p) \subseteq M_{k+2(p-1)}(\mathbb{F}_p) \subseteq \cdots.$$

The key fact about U_p is the following.

Theorem 15 (Théorème 6 in [2]).

(1) If $k > p+1$ then U_p sends $M_k(\mathbb{F}_p)$ to $M_{k'}(\mathbb{F}_p)$ for some $k' < k$.

(2) U_p is bijective on $M_{p-1}(\mathbb{F}_p)$.

Note that the k, k' in part (1) must be congruent mod $p-1$ by 5.

Proof. Part (1) follows from proposition 22(1) in the appendix. For part (2), it suffices to show that U_p is injective. Indeed, if $f \in M_{p-1}(\mathbb{F}_p)$ is nonzero, then either is is constant, in which case $f|U_p = f \neq 0$, or $w(f|U_p) = p-1$ so that $f|U_p \neq 0$. □

This theorem is truly remarkable. It says that if we take $f \in M_k(\mathbb{F}_p)$ and apply U_p repeatedly, it will move down the filtration of $M^k(\mathbb{F}_p)$ until it cannot anymore. At this point, it will be in $M_{k'}(\mathbb{F}_p)$ for some $k' \leq p+1$, which is finite dimensional. In particular, we have the following.

Proposition 16.

(1) For $\alpha \in \mathbb{Z}/(p-1)\mathbb{Z}$, there is a decomposition

$$M^\alpha(\mathbb{F}_p) = S^\alpha \oplus N^\alpha$$

so that U_p is nilpotent on N^α and bijective on S^α. Moreover, $S^\alpha \subset M_k(\mathbb{F}_p)$ such that $k \leq p+1$, so that S^α is finite dimensional.

(2) For $\alpha = 0$ we have $S^0 = M_{p-1}(\mathbb{F}_p)$.

The space S^α of the proposition is called the *ordinary space*. The map $e = \lim_{n\to\infty} U_p^{n!}$ projects $f \in M^\alpha(\mathbb{F}_p)$ onto S^α and is called the *ordinary projector*. Both of these objects will reappear in Katz's geometric formulation, where again the ordinary space will govern the limiting p-adic behavior of a modular form.

The simplest applications of this proposition occur when $M_k(\mathbb{F}_p)$ is as small as possible for all $k \leq p+1$.

Proposition 17. *Suppose $p \leq 7$. Then for all p-adic cusp forms $f \in M(\mathbb{Q}_p)$, we have*

$$\lim_{n\to\infty} f|U_p^n = 0.$$

(Recall that a modular form is a *cusp form* when its constant coefficient is 0.)

Proof. Scale f so that $f \in M(\mathbb{Z}_p)$. For $k < 12$ we know that $\dim M_k = 1$ with basis $\{E_k\}$. Therefore the only forms in $M_k(\mathbb{F}_p)$ with constant term 0 is 0 itself. Hence $\overline{f}|U_p^n = 0$ for n large enough. Dividing by $p^{v_p(f|U_p^n)}$ and repeating, we obtain the result. □

We can now demonstrate a strong sense in which the nonconstant terms of a p-adic modular form determine the constant term.

Proposition 18. *Suppose $p \leq 7$. If $f = \sum a_n q^n$ is a p-adic modular form of weight $k \neq 0$ then*

$$a_0 = \frac{1}{2}\zeta^*(1-k) \lim_{n\to\infty} a_{p^n}.$$

Proof. For these primes, we have $\zeta^*(1-k) \neq 0$. Therefore we can write $f = cG_k^* + g$ where g is a cusp form. Therefore it suffices to prove the proposition for $f = G_k^*$ and f a cusp form. For $f = G_k^*$ we have

$$\lim_{n\to\infty} a_{p^n} = \lim_{n\to\infty} \sigma_{k-1}^*(p^n) = \lim_{n\to\infty} 1 = 1$$

and $a_0 = \frac{1}{2}\zeta^*(1-k)$. And for f a cusp form, we have $\lim_{n\to\infty} f|U_p^n = 0$ by the preceding proposition. □

Remark 19. Let j again be the modular j-function. Although j has a pole at the cusp ∞, $j|U_p$ is a perfectly good q-expansion, as well as a weight 0 modular function (on $\Gamma_0(p)$, however, not $\mathrm{SL}_2(\mathbb{Z})$). Nevertheless, it ends up that $j|U_p$ *does* define a p-adic modular form of weight $\equiv 0 \pmod{p-1}$. Then for $p \leq 11$ we know that $M_{p-1}(\mathbb{F}_p) = \mathbb{F}_p$. Thus $(j-744)|U_p^n \to 0$, recovering the p-adic properties of j. Note that we've gotten one more prime than Lehner did: $p = 11$. In fact, $p = 11$ is the largest prime for which such congruences hold.

Appendix: filtrations

In this section, we discuss only $p \geq 5$.

Definition 20. For $f \in M(\mathbb{F}_p)$, we define the *filtration* $w(f)$ to be the minimal k such that f is the mod p reduction of a weight k modular form. That is,

$$w(f) = \min\{k : f \in M_k(\mathbb{F}_p)\}.$$

If $f \in M_k$, then $w(f)$ denotes $w(\overline{f})$.

Showing that two modular forms have different filtrations is a great way to show that they are not equal. Proving theorems about filtrations crucially relies on the fact that $E_{p-1} - 1$ is "the only relation" in $M(\mathbb{F}_p)$. We thus need the following structural facts about $M(\mathbb{F}_p)$.

Proposition 21.

(1) $M(\mathbb{F}_p) \cong \mathbb{F}_p[X,Y]/(\overline{A}-1)$ where $A \in \mathbb{Z}[X,Y]$ is such that $E_{p-1} = A(E_4, E_6)$.

(2) If $B \in \mathbb{Z}[X,Y]$ is such that $E_{p+1} = B(E_4, E_6)$ then $\overline{B}$ and $\overline{A}$ are coprime.

(3) $\overline{A}$ has no multiple-factors (i.e. it is square-free).

In Katz's theory, A will be replaced with the *Hasse invariant*.

Proposition 22. *Let f be a modular form.*

(1) $w(\Theta(f)) \leq w(f) + p + 1$ with equality if and only if $w(f) \not\equiv 0 \pmod{p}$.

(2) $w(f^i) = iw(f)$.

(3) $w(f|U_p) \leq p + \frac{w(f)-1}{p}$.

(4) If $w(f) = p-1$ then $w(f|U_p) = p-1$.

Proof. (1). Let the weight of f be $k = w(f)$. Since

$$\Theta(f) = \frac{\tilde{f} + kE_2 f}{12} \equiv \frac{\tilde{f} + kE_{p+1} f}{12} \pmod{p}$$

for some modular form $\tilde{f}$ of weight $k+2$ we have $w(f) \leq \max\{k+2, k+p+1\} = k+p+1$. If $p \nmid k$ then since $\overline{A}$ is coprime to $\overline{B}$, we get the equality case.

(2). This follows from $\tilde{A}$ having no multiple factors.

(3). Let the weight of f be $k = w(f)$, and set $k' = w(f|U_p)$. We have $(f|U_p)^p \equiv f - \Theta^{p-1}(f) \pmod{p}$, as one can easily check. Since $w(\Theta^{p-1}(f)) \leq k + p^2 - 1$ we have

$$pk' \leq k + p^2 - 1$$

as desired.

(4). Let f have weight $k = p-1$. Clearly $w(\Theta^2(f)) = 4$ or $p+3$. It cannot be 4 since the constant term of $\Theta^2(f)$ is 0. Thus $w(\Theta^2(f)) = p+3$. Applying part (1) gives $w(\Theta^{p-1}(f)) = p(p-1)$. From the formula $(f|U_p)^p \equiv f - \theta^{p-1}(f) \pmod{p}$ and part (2) we deduce $w(f|U_p) = p-1$. □

We are now ready to prove Theorem 6. The only additional input is that $M^0(\mathbb{F}_p)$ is integrally closed (in its field of fractions). This is ultimately a geometric fact.

Proof of Theorem 6 for $m \geq 2$. Replacing f' with $f'E_{(p-1)p^n}$ for n large enough, we may assume $h = k' - k \geq 4$. Setting $r = v_p(h) + 1$ we want to show that $r \geq m$. So suppose towards a contradiction that $r < m$. Then

$$fE_h - f' = f - f' + f(E_h - 1) \equiv 0 \pmod{p^r}$$

and

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

By Clausen-von Staudt, we have

$$p^{-r}(E_h - 1) = \lambda\phi$$

where $v_p(\lambda) = 0$ and $\phi = \sum_{n\geq 1} \sigma_{h-1} q^n$. Thus we have

$$\overline{\phi} = \frac{fE_h - f'}{\lambda f}$$

in the field of fractions of $M^0(\mathbb{F}_p)$.

Note now that

$$\phi - \phi^p \equiv \psi \pmod{p}$$

where

$$\psi = \sum_{(p,n)=1} \sigma_{h-1}(n) q^n \equiv -\frac{1}{24}\Theta^{h-1}(E_2) \equiv -\frac{1}{24}\Theta^{p-2}(E_{p+1}) \pmod{p}.$$

Hence $\overline{\psi} \in M^0(\mathbb{F}_p)$, so that ϕ is integral, and therefore in $M^0(\mathbb{F}_p)$.

But ϕ cannot be a modular form, for if it were then by taking the filtration of both sides of the equation above we would find

$$pw(\phi) = p^2 - 1$$

which is impossible as the RHS is not divisible by p. Contradiction. □

References

[1] Nicholas M. Katz, *p-adic properties of modular schemes and modular forms*, Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), 1973, pp. 69–190. Lecture Notes in Mathematics, Vol. 350.

[2] Jean-Pierre Serre, *Formes modulaires et fonctions zêta p-adiques*, Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972), 1973, pp. 191–268. Lecture Notes in Math., Vol. 350.