p-adic Modular Forms: An Introduction

Simon Spicer
0939537
Math 581G – Modular Forms and Hecke Operators
Fall 2011, University of Washington

December 13, 2011

1 Introduction

Conventional classical modular forms are defined over some finite extension of the rationals. One question that one can ask is if equivalent objects exist over the p-adics, in the sense that they truly reflect the p-adic topology and not just an extension of the base field.

Serre in the 1970s was the first to formalize such a question on the way to constructing p-adic L-functions, by way of developing the notion of a p-adic modular form to be the p-adic limit of some compatible family of q-expansions of classical modular forms. Katz came along fairly soon afterwards and generalized the theory to a much more geometric context, and showed that Serre's p-adic forms exist as a special case of a much wider family of p-adic objects. The theory has been further refined since then by Dwork, Hida, and most recently, Coleman, leading to the modern theory of overconvergent modular forms.

We will detail Serre's construction, prove one of the initial fundamental results, state two of the major theorems as outlined in his foundational paper [Se73], and give an example of a p-adic modular form. Katz's generalization of the theory will be mentioned briefly afterwards, but since it's exposition is somewhat more opaque than Serre's we will refrain from diving in too deeply here.

Unless otherwise stated in this paper p will denote a fixed rational prime ≥ 5. The cases of $p = 2$ and 3 require modified constructions in both Serre's and Katz's theory; for the sake of simplicity we will sometimes omit these. For more information, see [Go88, §1]

2 Serre's Construction

Serre was interested in developing the theory of p-adic L-functions, for which it sufficed to use a q-expansion-based construction of p-adic modular forms.

For ease of exposition we restrict ourselves to classical modular forms defined over $\mathbb{Q}$ and (p-adic forms over $\mathbb{Q}_p$) of level $N = 1$, although all the following results can be extended to forms of higher levels over number fields.

Definition 2.1. Let ν_p be the standard p-adic valuation on $\mathbb{Q}_p$, i.e. $\nu_p(\frac{r}{s}) = \mathrm{ord}_p(r) - \mathrm{ord}_p(s)$ for $\frac{r}{s} \in \mathbb{Q}$, and extend in the natural way. Let $f = \sum_n a_n q^n \in \mathbb{Q}[[q]]$ be a formal power series in q over $\mathbb{Q}$. Then we define

$$\nu_p(f) = \inf_n \nu_p(a_n).$$

Serre's construction is perhaps surprisingly elementary:

Definition 2.2. Let $\mathcal{M}_k$ be the space of modular forms of level 1 and weight k. A q-expansion

$$f = \sum_{n=0}^{\infty} a_n q^n \in \mathbb{Q}_p[[q]]$$

is a *Serre p-adic modular form* if there exists a sequence of classical modular forms $f_i \in \mathcal{M}_{k_i}$ such that

$$\nu_p(f - f_i) \to \infty \quad \text{as } i \to \infty.$$

Note that we do not require the f_i to have fixed weight; in fact, the following theorem will have as a corollary that that the weights k_i of the f_i converge p-adically in the nicest possible way.

Theorem 2.3. *Let f_1 and f_2 be two (classical) modular forms with coefficients in $\mathbb{Q}$ of weight k_1 and k_2 respectively, with $f_1, f_2 \neq 0$ and $\nu_p(f_1) = 0$. If there exists a positive integer m such that*

$$\nu_p(f_1 - f_2) \geq m,$$

then

$$\begin{aligned} k_1 &\equiv k_2 \quad (\mathit{mod}\ (p-1)p^{m-1}) \quad \mathit{if}\ p \geq 3, \\ k_1 &\equiv k_2 \quad (\mathit{mod}\ 2^{m-2}) \quad \mathit{if}\ p = 2. \end{aligned}$$

Proof. Serre's proof relies on the structure of the space of classical modular forms modulo p, as determined by Swinnerton-Dyer [SD73].
We provide a proof here for the case $m = 1$ i.e. $f_1 \equiv f_2 \pmod p \Rightarrow k_1 \equiv k_2 \pmod{p-1}$; for the full proof see [Se73, pp. 197-200].

We have three cases:

i $p = 2$

Trivial, since f_1 and f_2 are obviously congruent modulo 1.

ii $p = 3$:

Again trivial, since if $f_1, f_2 \neq 0$, then k_1 and k_2 must both be even (as nontrivial classical modular forms of level 1 exist only for even weights).

ii $p \geq 5$:

We will need a bit of background to prove this case.

Recall that the (classical) Eisenstein series E_k of weight k, normalized so that the constant coefficient is 1, has q-expansion

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

where B_k is the kth Bernoulli number, and

$$\sigma_r(n) = \sum_{d|n} d^r$$

is the rth power divisor function. In particular, let

$$\begin{aligned} Q &= E_4 = 1 - 240 \sum_{n \geq 1} \sigma_3(n) q^n \quad \text{and} \\ R &= E_6 = 1 - 504 \sum_{n \geq 1} \sigma_5(n) q^n. \end{aligned}$$

Definition 2.4. A polynomial is called *isobaric* if all monomials appearing in the polynomial have the same weight according to some given weight function on the indeterminates.

Let $\mathcal{M}$ be the graded algebra of classical modular forms over $\mathbb{Q}$, i.e.

$$\mathcal{M} = \bigoplus_k \mathcal{M}_k.$$

A standard result is that Q and R are algebraically independent and generate $\mathcal{M}$, i.e. $\mathcal{M} \simeq \mathbb{Q}[Q, R]$, and any $f \in \mathcal{M}_k$ can be written uniquely as the isobaric polynomial

$$f = \sum c_{a,b} Q^a R^b$$

for some finite set of pairs (a, b) such that $6a + 4b = k$; i.e. Q has weight 4 and R weight 6. For example, Ramanujan's Δ function, a cusp form of weight 12, is given by

$$\Delta = q \prod_{n \geq 1} (1 - q^n)^{24} = \frac{1}{1728}(Q^3 - R^2).$$

For $f \in \mathcal{M}_k$ such that $\nu_p(f) \geq 0$, we may consider $\tilde{f}$, the reduction of f modulo p, i.e

$$\tilde{f} = \sum_n \tilde{a}_n q^n \in \mathbb{F}_p[[q]],$$

where $\tilde{a}_n$ is just the nth Fourier coefficient of f reduced modulo p.

Let $\widetilde{\mathcal{M}}_k$ be the set of formal power series $\tilde{f}$ over $\mathbb{F}_p$, where f ranges over all $f \in \mathcal{M}_k$ such that $\nu_p(f) \geq 0$, and let

$$\widetilde{\mathcal{M}} = \sum_k \widetilde{\mathcal{M}}_k.$$

$\widetilde{\mathcal{M}}$ is called the *algebra of modular forms modulo p*.
Note that $\nu_p(Q) \geq 0$ and $\nu_p(R) \geq 0$, so $\widetilde{Q}, \widetilde{R} \in \widetilde{\mathcal{M}}$.
The proof that $f_1 \equiv f_2 \pmod p \Rightarrow k_1 \equiv k_2 \pmod{p-1}$ for $p \geq 5$ requires us to fully determine the structure of $\widetilde{\mathcal{M}}$.

Let $f = \sum c_{a,b} Q^a R^b$ be a modular form of weight k such that $\nu_p(f) \geq 0$. One can show then that the $c_{a,b}$ are all rational and $\nu_p(c_{a,b}) \geq 0$ (proven by induction on k, using that Δ is a linear combination of Q^3 and R^2 satisfying this condition).
Hence $\widetilde{\mathcal{M}}_k$ has as a basis the monomials $\widetilde{Q}^a \widetilde{R}^b$, where $6a + 4b = k$, and $\widetilde{\mathcal{M}}$ is generated by the reduced q-expansions $\widetilde{Q}$ and $\widetilde{R}$. However, these are no longer necessarily algebraically independent. That is, we have

$$\widetilde{\mathcal{M}} \simeq \mathbb{F}_p[X, Y]/\mathfrak{a}$$

for the ideal $\mathfrak{a} \subset \mathbb{F}_p[X, Y]$ of relations between $\widetilde{Q}$ and $\widetilde{R}$ i.e. those polynomials f for which $f(\widetilde{Q}, \widetilde{R}) = 0$.

<u>Claim</u>: The ideal $\mathfrak{a}$ is principal and generated by $A - 1$, where $A \in \mathbb{F}_p[X, Y]$ is the isobaric polynomial of weight $p - 1$ such that $A(\widetilde{Q}, \widetilde{R}) = \widetilde{E}_{p-1}$.

For example, in the case of $p = 7$, then $E_{p-1} = E_6 = R$, so the fundamental relation is $\widetilde{R} = 1$, and $\widetilde{\mathcal{M}} = \mathbb{F}_7[\widetilde{Q}]$.
And when $p = 11$ one has $E_{10} = QR$, so the fundamental relation is $\widetilde{Q}\widetilde{R} = 1$.

Recall that $E_{p-1} = 1 + \frac{2(p-1)}{B_{p-1}} \sum_{n \geq 1} \sigma_{p-2}(n) q^n$. We have that $\nu_p(B_{p-1}) = -1$ (see for example [BS67, p. 431]); hence $E_{p-1} \equiv 1 \pmod p$.
Let $\mathfrak{a}'$ be the ideal generated by $A - 1$. Then by the above $\mathfrak{a}' \subset \mathfrak{a}$, since by definition $A(\widetilde{Q}, \widetilde{R}) - \widetilde{E}_{p-1} = 0$. Furthermore, one can show that $A - 1$ is irreducible; hence $\mathfrak{a}'$ is prime.
Now since $\widetilde{\mathcal{M}}$ is an integral domain we have that $\mathfrak{a}$ is prime;
Also, $\mathfrak{a}$ is not maximal, since if it were $\widetilde{\mathcal{M}}$ would be finite, which it clearly is not (for example, the monomials $\widetilde{Q}\widetilde{R}$ of a given weight are linearly independent).
So let $\mathfrak{m}$ be a maximal ideal containing $\mathfrak{a}$. We then have the chain of prime ideals

$$0 \subset \mathfrak{a}' \subset \mathfrak{a} \subset \mathfrak{m}.$$

If $\mathfrak{a}' \neq \mathfrak{a}$ this would be a chain of length 3, violating the fact that $\overline{\mathcal{M}}$ is Krull dimension 2.
Hence $\mathfrak{a}' = \mathfrak{a}$, proving the claim.

Consider again $\mathbb{F}_p[X,Y]$ equipped with the grading where X has weight 4 and Y weight 6. Since $A-1$ has weight $p-1$, the ideal $\mathfrak{a}$ it generates is of weight 0 (mod $p-1$);
We may thus pass to the quotient and equip $\mathbb{F}_p[X,Y]$ with the grading of values in $\mathbb{Z}/(p-1)\mathbb{Z}$ (i.e. where the weights are reduced modulo $p-1$), and deduce that $\mathfrak{a}$ has weight 0 under this grading. Hence the quotient algebra $\widetilde{\mathcal{M}} = \mathbb{F}_p[X,Y]/\mathfrak{a}$ is graded with degree group $\mathbb{Z}/(p-1)\mathbb{Z}$. We conclude that

$$\widetilde{\mathcal{M}} = \bigoplus_{\alpha\in\mathbb{Z}/(p-1)\mathbb{Z}} \widetilde{\mathcal{M}}^\alpha, \text{ where } \widetilde{\mathcal{M}}^\alpha = \bigcup_{k\equiv\alpha \pmod{p-1}} \widetilde{\mathcal{M}}_k.$$

Finally, we return to our modular forms f_1 and f_2 such that $f_1 \equiv f_2 \pmod p$, i.e. $\tilde{f}_1 = \tilde{f}_2$. But then the above decomposition of $\widetilde{\mathcal{M}}$ yields that $\exists\ \alpha \in \mathbb{Z}/(p-1)\mathbb{Z}$ such that $\tilde{f}_1 = \tilde{f}_2 \in \widetilde{\mathcal{M}}^\alpha$. Thus $k_1 \equiv k_2 \pmod{p-1}$, completing the proof.

□

Let us now define

$$X_m = \begin{cases} \mathbb{Z}/(p-1)p^{m-1}\mathbb{Z} & p \geq 3 \\ \mathbb{Z}/2^{m-2}\mathbb{Z} & p = 2 \end{cases}$$

$$\text{and } X = \varprojlim_m X_m \simeq \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z} \quad \text{by the Chinese Remainder Theorem,}$$

then we obtain the following beautiful corollary of the above theorem, the first nontrivial property Serre p-adic modular forms:

Corollary 2.5. *Let f be a Serre p-adic modular form and f_i a sequence of classical modular forms with coefficients in $\mathbb{Q}$ and weights k_i that converge p-adically to f. Then there exists a unique $k \in X$ such that k_i converges to k. Moreover, k is independent of the choice of f_i. We call k the* **weight** *of f.*

Proof. Since $\nu_p(f - f_i) \to \infty$ the above theorem holds, and we may set $k = \varprojlim k_i$. Then $k \in X$ by definition, and is unique and independent of the specific choice of f_i by standard results.

□

A useful result is that in order to construct a Serre p-adic modular form, it suffices to obtain a family f_i of classical modular forms of compatible weights whose a_n converge uniformly for $n \geq 1$; i.e. having done so we get the constant term 'for free'. The result is formalized in the following:

Theorem 2.6 (Serre)**.** *Let $f_i = \sum_{n\geq 0} a_{i,n}q^n$ be a sequence of p-adic modular forms of weights k_i such that*

- *for $n \geq 1$, the $a_{i,n}$ converge uniformly to some $a_n \in \mathbb{Q}_p$,*
- *k_i converge to some $k \in X$.*

Then

- *$a_{0,n}$ converge to some $a_0 \in \mathbb{Q}_p$,*
- *$f = \sum_{n\geq 0} a_n q^n$ is a Serre p-adic modular form of weight k.*

Example 2.7. Using this theorem, we can construct an example of a Serre p-adic modular form from the familiar Eisenstein series. Recall that the Eisenstein series G_k of weight k is given by

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

where B_k is the kth Bernoulli number, and $\sigma_r(n) = \sum_{d|n} d^r$ the rth power divisor function. Let X be defined as before, $k \in X$ and $n \in \mathbb{N}_{\geq 1}$. Observe that if d is a positive integer, then $d^{k-1} \in \mathbb{Z}_p$, so we may define

$$\sigma^*_{k-1}(n) = \sum_{\substack{d|n \\ \gcd(n,p)=1}} d^{k-1} \in \mathbb{Z}_p.$$

So choose $k \in X$ is even and nonzero. Then we may certainly find a sequence $k_i \geq 4$ of positive even integers whose archimedian absolute value tends to infinity and $k_i \to k$ p-adically. We then have that for positive integer d coprime to p, $d^{k_i-1} \to d^{k-1}$. in the p-adic norm. Hence

$$\sigma^*_{k-1}(n) = \varprojlim_i \sigma_{k_i-1}(n) \in \mathbb{Z}_p,$$

and this convergence is uniform over all $n \geq 1$.

Thus by the above theorem, the G_{k_i} converge to a p-adic modular form of weight k, called G^*_k, the p-adic Eisenstein series of weight k, and

$$G^*_k = \left(\varprojlim_i -\frac{B_k}{2k}\right) + \sum_{n=1}^{\infty} \sigma^*_{k-1}(n)q^n.$$

Interestingly, the weight 2 p-adic Eisenstein series is a p-adic modular form even though the classical weight 2 Eisenstein series is not a classical modular form.

3 Katz's Generalization

In 1973 Katz reformulated the notion of a p-adic modular form from a much more modular point of view. Recall that classical meromorphic modular forms can be thought of as functions on triples $(E/\mathbb{Z}, \omega, \iota)$, where E is an elliptic curve over the ring $\mathbb{Z}$, ω a nonvanishing differential on E, and ι a level structure on E obeying some prescribed transformation laws. If one were to simply copy this definition but let the base ring be $\mathbb{Z}_p$, we simply get $\mathbb{Z}_p$ tensored with the classical modular forms over $\mathbb{Z}$ [Go88, pg.1].

However, we can define a notion of a truly p-adic modular form by introducing soothing called the *growth condition*. Katz's definition of a p-adic modular form can be thought of as a function on quadruples of an elliptic curve over a p-adic ring, a nonvanishing differential thereon, a level structure, and a p-adic constant relating the elliptic curve to the prescribed growth condition. We will simply state the formal definition of such a p-adic modular form here and leave it at that, since developing the theory beyond this is a non-trivial matter.

We begin by defining *test objects*, the tuples on which these p-adic modular forms will operate. For this we observe that the Eisenstein series $E_{p-1}(E, \omega)$ of weight $p-1$ may be interpreted as functions of pairs of elliptic curves and non-vanishing differentials thereon.

Definition 3.1. Let B be a p-adic ring, and A a complete separated B-algebra. Let $r \in B$ be a constant, and $\Gamma_1(N)$ the usual congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. We define a **test object of level N and growth condition r over B** to be a quadruple

$$(E/A, \omega, \iota, Y),$$

where E is an elliptic curve over A, ω a nonvanishing differential on E, ι a $\Gamma_1(N)$-invariant structure on E, and $Y \in A$ the value satisfying

$$Y \cdot E_{p-1}(E, \omega) = r.$$

Definition 3.2 (Katz)**.** A *p-adic modular form over B of weight k, level N and growth condition r* is a rule f which assigns a value in A to a test object $(E/A, \omega, \iota, Y)$ over B of level N and growth condition r, i.e.

$$f(E/A, \omega, \iota, Y) \in A,$$

subject to the following conditions:

i $f(E/A, \omega, \iota, Y)$ depends only on the isomorphism class of $(E/A, \omega, \iota)$;

ii $f(E/A, \omega, \iota, Y)$ commutes with base change;

iii for any $\lambda \in A^*$ we have

$$f(E/A, \omega, \iota, \lambda^{1-p} Y) = \lambda^{-k} f(E/A, \omega, \iota, Y).$$

The space of p-adic modular forms over B of weight k, level N and growth condition r is denoted

$$F(B, k, N, r).$$

Note that since the space is truly p-adic we immediately have that

$$\varprojlim_n F(B/p^n B, k, N, r) = F(B, k, N, r).$$

The introduction of the growth condition r is equivalent to restricting consideration away from disks of supersingular curves of radius r. When $r = 1$ we only consider ordinary curves, and Katz shows this case is equivalent to Serre's formulation (see [Ka83]). However, setting r to be a p-adic unit other than 1 allows for the notion of "overconvergent" p-adic modular forms, for which there is no analogy in Serre's theory.

Finally, one should note that the theory of p-adic modular forms has been developed considerably since Katz's paper, which was published in the early 1980s. Notably, Coleman's notion of overconvergent modular forms (for example see [Co96]) further develops Katz's modular approach.

References

[BS67] Z. I. Boreviĉ and I. R. Shafareviĉ. *Théorie des nombres* (translated from Russian by M. and JL. Verley), Gauthier-Villars, Paris, 1967.

[Co96] R.Coleman. *Classical and overconvergent modular forms.* Invent. Math. 124 (1996), pp. 215-224

[Go88] F. Gouvêa. *Arithmetic of p-adic modular forms.* Lecture Notes in Mathematics 1304, Springer-Verlag, 1988, MR1027593.

[Ka83] N.M. Katz. *p-adic Properties of Modular Schemes and Modular Forms.* In "Modular functions of one variable, III", Lecture Notes in Mathematics 350, Springer-Verlag, 1983, pp. 69190, MR0447119.

[Se73] J.-P. Serre. *Formes modulaires et fonctions zêta p-adiques.* in "Modular functions of one variable, III", Lecture Notes in Mathematics 350, Springer-Verlag, 1973, pp. 191268, MR0404145.

[SD73] P. Swinnerton-Dyer. *On ℓ-adic representations and congruences for coefficients of modular forms.* in "Modular functions of one variable, III", Lecture Notes in Mathematics 350, Springer-Verlag, 1973, pp. 1-55, MR0406931.