p-adic modular forms

TCC (Spring 2021), Lecture 8

Pak-Hin Lee

11th March 2021

Administrative issues

Slides:

- Lectures 1-7: available on webpage

Problem sheets:

- Problem Sheet 3: available later, due two weeks after being posted

Office hours:

- 12th March (Friday): 5 pm to 6 pm
- 18th March (Thursday): usual class time, details TBA

Plans

Today (survey style):

- Recap of p-adic modular forms
- Hecke operators
- Canonical subgroups
- Spectral theory

Recap: *p*-adic modular forms with growth conditions

- Fix a *p*-adically complete ring R_0 and $r \in R_0$.
- r-test object: $(E/R, \omega, \alpha_N, Y)$ where R is an R_0-algebra in which p is nilpotent, and $Y \cdot E_{p-1}(E/R, \omega) = r$.
- *p*-adic modular forms over R_0 of growth r, level N and weight k: $f \in M(R_0; r, N, k)$ is a rule on r-test objects.

Idea

We only consider test objects which are not "too supersingular":

- $|r| = 1$: ordinary locus (with supersingular disks removed) $\rightsquigarrow$ convergent *p*-adic modular forms;
- $|r| < 1$: thickening of ordinary locus (extending across the boundary of supersingular disks) $\rightsquigarrow$ overconvergent *p*-adic modular forms.

Moduli interpretation: $p \in R_0$ nilpotent

Suppose p is nilpotent in R_0, and N is such that E_{p-1} exists. Set $\mathcal{L} := \underline{\omega}^{\otimes(1-p)}$.

Proposition

The moduli problem

$$R_0\text{-scheme } S \rightsquigarrow \{(E/S, \alpha_N, Y)\}/\sim$$

(with notation as in the previous remark) is representable by the affine scheme

$$Y^{(r)}(N) := \mathrm{Spec}_{Y(N)_{R_0}}\left(\mathrm{Sym}(\mathcal{L}^\vee)/(E_{p-1} - r)\right).$$

Remark

The affine curve $Y(N)_{R_0}$ represents $\{(E/S, \alpha_N)\}$.

Moduli interpretation: $p \in R_0$ nilpotent

As before, this implies we can work geometrically:

Proposition

$$M(R_0; r, N, k) = H^0(Y^{(r)}(N), \underline{\omega}^{\otimes k}).$$

As a corollary, we obtain an anologue of Swinnerton-Dyer's result on mod p modular forms:

Corollary

$$M(R_0; r, N, k) = \left(\bigoplus_{j \geq 0} M(R_0; N, k + j(p-1)) \right) / (E_{p-1} - r).$$

Remark

This corrects a typo from Lecture 7.

Moduli interpretation

- For general R_0, recall that

$$M(R_0; r, N, k) = \varprojlim_m M(R_0/p^m R_0; r, N, k).$$

- When $r = 1$,

$$Y^{(1)}(N) = Y(N) - \{E_{p-1} = 0\} =: Y(N)^{\mathrm{ord}}$$

is the ordinary locus and the space of p-adic modular forms is given by

$$M(\mathbf{Z}_p; 1, N, k) = \varprojlim_m H^0(Y(N)^{\mathrm{ord}} \otimes \mathbf{Z}/p^m\mathbf{Z}, \underline{\omega}^{\otimes k}).$$

- Next we will see that this agrees with Serre p-adic modular forms of integral weights k.

Relation with Serre p-adic modular forms

Proposition (Imprecise form of Proposition 2.7.2)

$f \in M(\mathbf{Z}_p; 1, N, k)$ if and only if there exists a sequence $f_m \in M(\mathbf{Z}_p; N, k_m)$ such that $k_m \to k$ in $\mathfrak{X}$ and their q-expansions converge $f_m \to f$.

Proof sketch:

- Given $f \in M(\mathbf{Z}_p; 1, N, k)$, we have

$$f \pmod{p^m} \in H^0((Y(N) \otimes \mathbf{Z}/p^m\mathbf{Z})[E_{p-1}^{-1}], \underline{\omega}^{\otimes k}).$$

- This can be written as $\dfrac{g_m}{E_{p-1}^{\alpha_m}}$, where

$$\begin{aligned} g_m &\in H^0(Y(N) \otimes \mathbf{Z}/p^m\mathbf{Z}, \underline{\omega}^{\otimes(k+\alpha_m(p-1))}) \\ &= H^0(Y(N)_{\mathbf{Z}_p}, \underline{\omega}^{\otimes(k+\alpha_m(p-1))}) \otimes \mathbf{Z}/p^m\mathbf{Z}. \end{aligned}$$

Relation with Serre p-adic modular forms

- Multiplying g_m by a higher power of E_{p-1} if necessary, we can assume
$$\alpha_m \equiv 0 \pmod{p^m}.$$
- The converse is easier.
- For precise statements and proofs, see [Katz, §2.7].

An example

Example

Let $p = 5$ and $N = 1$.

- There is only one supersingular point in char 5, since $E_4 \equiv A \pmod 5$.
- The modular curve does not exist, but we can consider $X = \mathbf{P}^1_{j,\mathbf{Z}_p}$ where $j = \frac{E_4^3}{\Delta}$.
- The ordinary locus is

$$X^{\mathrm{ord}} = \mathbf{P}^1_{j,\mathbf{Z}_p} - \{E_4 = 0\} = \operatorname{Spec} \mathbf{Z}_p[\frac{1}{j}] = \mathbf{A}^1_{j,\mathbf{Z}_p}.$$

- For simplicity, consider the spaces of weight 0 modular forms

$$M(R) := M(R; r = 1, N = 1, k = 0).$$

An example

Example (continued)

- Then the fibers $X^{\mathrm{ord}} \otimes \mathbf{Z}/p^m\mathbf{Z}$ give

$$M(\mathbf{Z}/p^m\mathbf{Z}) = H^0(X^{\mathrm{ord}} \otimes \mathbf{Z}/p^m\mathbf{Z}, \mathcal{O}) = (\mathbf{Z}/p^m\mathbf{Z})[\frac{1}{j}].$$

- Note that we don't want $M(\mathbf{Z}_p)$ to be

$$H^0(X^{\mathrm{ord}}_{\mathbf{Z}_p}, \mathcal{O}) = \mathbf{Z}_p[\frac{1}{j}]$$

  but it should be

$$\varprojlim_m M(\mathbf{Z}/p^m\mathbf{Z}) = \mathbf{Z}_p\langle\frac{1}{j}\rangle.$$

- This illustrates why p has to be nilpotent in the definition.

Hecke operators

Classical theory (over $\mathbf{C}$):

- modular forms: functions on lattices $\Lambda \subset \mathbf{C}$
- Hecke operators T_ℓ: averaging over sublattices $\Lambda' \subset \Lambda$ of index ℓ

Moduli interpretation (over any ring R):

- For a prime ℓ and test object (E, ω), let $C \subset E$ be any finite flat subgroup scheme of order ℓ defined over R.
- Consider $\pi : E \to E/C$ (an isogeny of degree ℓ) and the dual isogeny $\pi^\vee : E/C \to E$.
- ω on E pulls backs to $(\pi^\vee)^*\omega$ on E/C.
- $(E/C, (\pi^\vee)^*\omega)$ is a test object if ℓ is invertible in R.
- Level structures can be incorporated if $\ell \nmid N$.

Hecke operators

For f a modular form of weight k, define $T_\ell f$ by

$$(T_\ell f)(E, \omega) := \ell^{k-1} \sum_C f(E/C, (\pi^\vee)^* \omega)$$

where C runs through the $\ell + 1$ subgroups of $E[\ell]$ of order ℓ.

Remark

Technical issues (which can be ignored for now):

1. One has to pass to an extension $R \subset R'$ to trivialize $E[\ell]$ in the étale topology.
2. Show that $T_\ell f$ is independent of the choices of C.
3. Show that $T_\ell f$ is defined over R.

Tate curve

Consider Tate(q) over $\mathbf{Z}((q))$. View this as $\mathbf{G}_m/q^{\mathbf{Z}}$, so the order ℓ subgroups are

$$\mu_\ell = \langle \zeta \rangle \quad \text{and} \quad H_i := \langle \zeta^i q^{1/\ell} \rangle, i = 0, 1, \cdots, \ell - 1.$$

For μ_ℓ:

- Tate(q)$/\mu_\ell \cong$ Tate(q^ℓ) is induced by $X \mapsto X^\ell$.
- Dual $\pi^\vee$: Tate(q^ℓ) $\to$ Tate(q) is induced by quotienting $q^{\mathbf{Z}}$.
- Hence $(\pi^\vee)^*(\omega_{\mathrm{can}}) = \omega_{\mathrm{can}}$.

For H_i:

- Tate(q)$/H_i \cong$ Tate($\zeta^i q^{1/\ell}$).
- Dual $\pi^\vee$: Tate($\zeta^i q^{1/\ell}$) $\to$ Tate(q) is induced by $X \mapsto X^\ell$.
- Hence $(\pi^\vee)^*(\omega_{\mathrm{can}}) = \ell\omega_{\mathrm{can}}$ (check: $\frac{du}{u} \mapsto \frac{d(u^\ell)}{u^\ell} = \ell \cdot \frac{du}{u}$).

q-expansions of Hecke operators

- Using these, it is straightforward to compute the q-expansions: If

$$f(\mathrm{Tate}(q), \omega_{\mathrm{can}}) = \sum_i a_i q^i,$$

then

$$(T_\ell f)(\mathrm{Tate}(q), \omega_{\mathrm{can}}) = \sum_i \left(\ell^{k-1} a_{i/\ell} + a_{\ell i}\right) q^i.$$

- See [Katz, §1.11] for details about Hecke operators.

Remark

- The subgroups μ_ℓ and H_i play different roles: μ_ℓ is "distinguished".
- There is a similar story in the p-adic setting.

Supersingular elliptic curves

Before introducing the canonical subgroup, we need to study supersingular elliptic curves.
Notation:

- Consider a finite extension $K/\mathbf{Q}_p$, with ring of integers $R = \mathcal{O}_K$ and valuation $v : \mathcal{O}_K - \{0\} \to \mathbf{Q}_{\geq 0}$ (normalized such that $v(p) = 1$).
- Let $S = R/pR$. Then v induces

$$v : S - \{0\} \to [0, 1) \cap \mathbf{Q}$$

satisfying $v(ur) = v(r)$ for $u \in S^\times$.

Remark

S may contain nilpotents! In fact, we will see that the theory is almost vacuous if S is reduced (i.e. $K/\mathbf{Q}_p$ is unramified).

Supersingular elliptic curves

Let E/K be an elliptic curve with good reduction.

- There is a model $\mathcal{E}/R$, and hence $\overline{E}/S$.
- Consider the Hasse invariant

$$A(\overline{E},\omega) \in S,$$

where $\omega \in H^0(\overline{E},\Omega^1_{\overline{E}/S})$ is a basis (unique up to $S^\times$).

Two cases:

1. $A(\overline{E},\omega) = 0$: We say E is "very supersingular".
2. $A(\overline{E},\omega) \neq 0$: We say E is "not too supersingular" and define

$$v(E) := v(A(\overline{E},\omega)) \in [0,1) \cap \mathbf{Q}.$$

Supersingular elliptic curves

Thus $v(E) \in [0,1)$ measures how supersingular E is:

- $v(E) = 0$: E has ordinary reduction.
- $v(E) > 0$: E has supersingular reduction.
- The larger $v(E)$ is, the "more supersingular" E is.

Given a test object $(E/R, \omega)$,

$$\begin{aligned} & (E/R,\omega) \text{ can be upgraded to an } r\text{-test object} \\ \iff & Y \cdot E_{p-1}(E,\omega) = r \text{ has a solution} \\ \iff & v(E) \leq v(r). \end{aligned}$$

Canonical subgroups: ordinary case

Let $R = \mathcal{O}_K$ with residue field k, and E/R be an elliptic curve.

- $E(\overline{K})[p] \cong (\mathbf{Z}/p\mathbf{Z})^2$ contains $p+1$ subgroups of order p. We shall see that $E[p]$ contains a "canonical" subgroup of order p in certain cases.
- If E has ordinary reduction, then $E(\overline{k})[p] \cong \mathbf{Z}/p\mathbf{Z}$, so the kernel of
$$E(\overline{K})[p] \to E(\overline{k})[p]$$
is a cyclic subgroup of $E(\overline{K})$ of order p; this is the canonical subgroup of E.
- If E has supersingular reduction, then $E(\overline{k})[p] = 0$, so the reduction map above gives no information. However, we will see that E has a canonical subgroup when it is "not too supersingular".

Canonical subgroups: $p = 2$

Let us illustrate everything explicitly when $p = 2$:

subgroups of order 2 $\longleftrightarrow$ non-trivial 2-torsion points!

Every elliptic curve has a minimal Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in R.$$

Completing the square gives

$$\left(y + \frac{a_1x}{2} + \frac{a_3}{2}\right)^2 = x^3 + \left(a_2 + \frac{a_1^2}{4}\right)x^2 + \left(a_4 + \frac{a_1a_3}{2}\right)x + \left(a_6 + \frac{a_3^2}{4}\right).$$

Idea

A **canonical** root is the unique root of the RHS of minimal valuation.

Canonical subgroups: $p = 2$

By an exercise with the Newton polygon:

- If $v(a_1) \geq \frac{2}{3}$, then all roots have valuation $-\frac{2}{3}$.
- If $v(a_1) < \frac{2}{3}$, then there is a unique root with minimal valuation $2(v(a_1) - 1)$.

See the beginning of [Calegari, §3] for details.
Moreover:

Lemma

$a_1 \mod 2$ *is the Hasse invariant of* E *over* $R/2$.

Canonical subgroups

Theorem (Lubin–Katz)

Let R be a p-adically complete DVR with $v(p) = 1$, and $S = R/pR$. Then an elliptic curve E/R has a canonical subgroup of order p if and only if

$$v(A(E_S, \omega_S)) < \frac{p}{p+1},$$

where A is the Hasse invariant (over S).

The proof uses formal groups and is carried out in [Katz, §3.4–3.9]. For many applications, it is not necessary to know the proof!

Remark

If p is unramified in R, $v(E) < \frac{p}{p+1}$ forces $v(E) = 0$, so E must have ordinary reduction.

Modular forms of level p as p-adic modular forms

Using the canonical subgroup, we can view classical modular forms of level p as p-adic modular forms:

- Suppose $v(r) < \frac{p}{p+1}$.
- If $(E/R, \omega, Y)$ is an r-test object, then

$$v(E) \leq v(r) < \frac{p}{p+1},$$

  so E has a canonical subgroup H.
- This gives rise to a (classical) test object $(E/R, \omega, H)$ of level $\Gamma_0(p)$.

Remark

Unfortunately we have not defined $\Gamma_0(p)$-level properly; see [Katz, §1.3 & §1.13].

Modular forms of level p as p-adic modular forms

- Thus we get a map

$$\{r\text{-test objects } (E/R, \omega, Y)\} \to \left\{\begin{matrix}\text{test objects } (E/R, \omega, H) \\ \text{of level } \Gamma_0(p)\end{matrix}\right\},$$

  which induces

$$\left\{\begin{matrix}\text{classical modular forms} \\ \text{of level } \Gamma_0(p)\end{matrix}\right\} \to \left\{\begin{matrix}p\text{-adic modular forms of} \\ \text{growth } r \text{ and level } 1\end{matrix}\right\}.$$

- See [Katz, Theorem 3.2] for details.
- Moreover, this map respects the (classical) U_p-operator on LHS and the (p-adic) U_p-operator on RHS, to be defined next.

U and V operators

In Serre's theory, the U and V operators are defined on the level of power series. The canonical subgroup provides a more conceptual framework:

- Suppose $v(r) < \frac{p}{p+1}$, so that every r-test object $(E/R, \omega, Y)$ has a canonical subgroup $H \subset E[p]$.
- Define
$$(V_p f)(E, \omega, Y) = f(E/H, \cdots)$$
and
$$(U_p f)(E, \omega, Y) = p^{k-1} \sum_{\substack{C \subset E[p] \\ C \neq H}} f(E/H, \cdots).$$

Remark

For now we are neglecting how the growth condition behaves; this is crucial!

U and V operators

- In terms of q-expansions, if $f = \sum a_n q^n$, then
$$V_p f = \sum a_n q^{np}$$
and
$$U_p f = \sum a_{np} q^n.$$
- Clearly $U_p V_p$ is the identity.

U and V operators

To see how U and V affect the growth condition, it is necessary to understand how $v(E)$ behaves under quotients.

Proposition

Suppose E has $v(E) < \frac{p}{p+1}$ and canonical subgroup H. Then

1. *If C is a subgroup of order n with $(n, p) = 1$, then $v(E/C) = v(E)$.*
2. *If $C \neq H$ is a subgroup of order p, then $v(E/C) = \frac{1}{p}v(E)$.*
3. *If $v(E) < \frac{1}{p+1}$, then $v(E/H) = pv(E)$.*

U and V operators

Now we are ready to specify how U and V act on p-adic modular forms with growth condition r (of a fixed weight and level). Denote this space by $M[r]$.

Theorem

Suppose $v(r) < \frac{1}{p+1}$. Then:

1. $U_p : M[r] \to M[r^p]$.
2. $V_p : M[r^p] \to M[r]$.

Slogan: U_p improves overconvergence.

Remark

Strictly speaking, these are true over a field, but are more subtle over integral coefficients; see [Katz, Theorem 3.3 & §3.10-3.12].

Spectrum of U

Consider $r = 1$ and the space M of (convergent) p-adic modular forms.

- Let $f \in M$ and set $g = (1 - V_p U_p) f$.
- For $|\lambda| < 1$, check that

$$f_\lambda = \sum_{i=0}^{\infty} (\lambda V_p)^i g \in M$$

  satisfies $U_p f_\lambda = \lambda f_\lambda$ (Problem Sheet 3).
- **Conclusion:** The one-parameter family f_λ consists of eigenvectors. In other words, U_p has a continuous spectrum on M.

Spectrum of U

- There are too many **convergent** p-adic modular forms (for $v(r) = 0$).
- On the other hand, the spectral theory for U_p on **overconvergent** modular forms $M[r]$ (for $v(r) > 0$) is better-behaved.

Theorem

Suppose $0 < v(r) < \frac{p}{p+1}$. Then $U_p : M[r] \to M[r]$ is a compact operator.

This implies U_p has a discrete spectrum on $M[r]$.

Spectrum of U

Example

Let $p = 5$, $N = 1$ and $k = 0$. Suppose $v(r) > 0$, i.e. $|\frac{1}{r}| > 1$. Then

$$M[1] = \left\{ \text{convergent power series on } |\frac{1}{j}| \leq 1 \right\},$$
$$M[r] = \left\{ \text{convergent power series on } |\frac{1}{j}| \leq |\frac{1}{r}| \right\}.$$

Note $M[1] \supset M[r] \supset M[r']$ whenever $0 < v(r) < v(r')$.

See:

- [Katz, §3.13] for applications to congruences for j;
- [Calegari, §3] for a systematic account of the spectral theory for U_p.