p-adic modular forms

TCC (Spring 2021), Lecture 7

Pak-Hin Lee

4th March 2021

Administrative issues

Slides:

- Lectures 1-6: available on webpage
- Lecture 6: extra discussion about Tate uniformization

Problem sheets:

- 3 sets for assessment
  1. 22nd February (Monday of Week 6): posted
  2. 8th March (Monday of Week 8): posted
  3. 22nd March (Monday of Week 10): tentative
- available at least two weeks before deadlines

Administrative issues

Office hours:

- Dates: 2nd, 9th, 16th March (Tuesdays)
- Time: 12 pm to 1 pm
- Format: Q&A, possibly supplementary lectures

References for geometric modular forms:

- Calegari's AWS notes, 2013
- Loeffler's TCC notes, 2014
- Katz, §1 and Appendix 1
- I am happy to answer questions about these!

Plans

Today:

- Recap of geometric modular forms
- q-expansion principle and base change
- Hasse invariant
- p-adic modular forms

Next week: a subset of

- Hecke operators
- Canonical subgroups
- Spectral theory
- Further topics

Example: E_4 and E_6

Suppose $\frac{1}{6} \in R_0$. Then any pair $(E/R, \omega)$ can be written in terms of Weierstrass equation

$$\left(y^2 = 4x^3 + a_4 x + a_6, \frac{dx}{y}\right).$$

Then the rules

$$E_4(E/R, \omega) := -12a_4,$$
$$E_6(E/R, \omega) := 216a_6$$

define modular forms of weights 4 and 6 respectively, so

$$E_4 \in M(R_0; 1, 4), \quad E_6 \in M(R_0; 1, 6);$$

here R_0 can be taken to be $\mathbf{Z}[\frac{1}{6}]$ (in fact $\mathbf{Z}$, as we will see).

Example: E_4 and E_6

Evaluating at the Tate curve gives the q-expansions

$$E_4(\mathrm{Tate}(q), \omega_{\mathrm{can}}) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n \in \mathbf{Z}[[q]],$$

$$E_6(\mathrm{Tate}(q), \omega_{\mathrm{can}}) = 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) q^n \in \mathbf{Z}[[q]].$$

By the q-expansion principle (to be discussed next), E_4 and E_6 are holomorphic modular forms defined over $\mathbf{Z}$:

$$E_4 \in S(\mathbf{Z}; 1, 4), \quad E_6 \in S(\mathbf{Z}; 1, 6).$$

See Problem Sheet 3.

Remark

In general, $E_k \in S(\mathbf{Q}; 1, k)$ for even $k \geq 4$.

Recap: Modular curves

- A level N structure on E/S is an isomorphism of group schemes $\alpha_N : E[N] \xrightarrow{\sim} (\mathbf{Z}/N\mathbf{Z})^2_S$.
- For $N \geq 3$, the moduli problem

$$S \text{ scheme over } \mathbf{Z}[\frac{1}{N}] \rightsquigarrow \{(E/S, \alpha_N)\}/\sim$$

  is represented by a (fine) moduli scheme $Y(N)$ over $\mathbf{Z}[\frac{1}{N}]$.
- $Y(N)$ has a "natural compactification" $X(N)$.
- Refer to [Loeffler, §3] for the formalism of moduli spaces and representable functors.
- For instance, $Y(N)(\mathbf{C})$ is a disjoint union of $\varphi(N)$ copies of $\Gamma(N)\backslash\mathbf{H}$.
- The level N structures on $\text{Tate}(q^N)$ correspond to the cusps of $X(N)$.

q-expansion principle

Recall that we have defined for any $\mathbf{Z}[\frac{1}{N}]$-module R

$$S(R; N, k) := H^0(X(N), \underline{\omega}^{\otimes k} \otimes_{\mathbf{Z}[\frac{1}{N}]} R);$$

this agrees with the ruled-based definition when R is a ring.

Theorem (q-expansion principle)

Let $N \geq 3$. Suppose $L \subset K$ are $\mathbf{Z}[\frac{1}{N}]$-modules, and $f \in S(K; N, k)$. Suppose that for each geometrically connected component of $X(N)$, there is at least one cusp at which the q-expansion of f has coefficients in $L \otimes_{\mathbf{Z}[\frac{1}{N}]} \mathbf{Z}[\frac{1}{N}, \zeta_N]$. Then f is a modular form with coefficients in L.

The proof requires non-trivial use of algebraic geometry.

Remark

With some care, this is also valid for level 1 and 2.

Base-change of modular forms

- In the classical setting, the space of modular forms over $\mathbf{C}$ has a rational or even integral structure.
- Base-change theorems give similar results for geometric modular forms.

Base-change: level $N \geq 3$

Theorem

Suppose either:

- $N \geq 3$, $k \geq 2$; *or*
- $3 \leq N \leq 11$, $k = 1$.

Then for any $\mathbf{Z}[\frac{1}{N}]$*-module* K*, there is an isomorphism*

$$S\left(\mathbf{Z}[\frac{1}{N}]; N, k\right) \otimes_{\mathbf{Z}[\frac{1}{N}]} K \xrightarrow{\sim} S(K; N, k).$$

Idea of proof.

- Identify $S(K; N, k) = H^0(X(N), \underline{\omega}^{\otimes k} \otimes_{\mathbf{Z}[\frac{1}{N}]} K)$.
- Use cohomology and base-change, and show $H^1(X(N), \underline{\omega}^{\otimes k}) = 0$. □

Base-change: level 1 and 2

Theorem

Suppose $N = 1$ (resp. $N = 2$), $k \geq 1$ and R is any ring with $\frac{1}{6} \in R$ (resp. $\frac{1}{2} \in R$). Then there is an isomorphism

$$S(\mathbf{Z}; N, k) \otimes_{\mathbf{Z}} R \xrightarrow{\sim} S(R; N, k).$$

Idea of proof.

Identify level 1 modular forms as the fiber product:

$$\begin{array}{ccc} S(R;3,k) & \longleftarrow & S(R;1,k) \\ \downarrow & \square & \downarrow \\ S(R;12,k) & \longleftarrow & S(R;4,k) \end{array}$$

□

Base-change: level 1 and 2

The condition that 6 is invertible is crucial:

Example

Later we will study the Hasse invariant $A \in S(\mathbf{F}_p; 1, p-1)$.

1. $p = 2$: $A \in S(\mathbf{F}_2; 1, 1)$ but $S(\mathbf{Z}; 1, 1) = 0$.
2. $p = 3$: $A \in S(\mathbf{F}_3; 1, 2)$ but $S(\mathbf{Z}; 1, 2) = 0$.

Hence for $p = 2, 3$, the map

$$S(\mathbf{Z}; 1, k) \otimes_{\mathbf{Z}} \mathbf{F}_p \to S(\mathbf{F}_p; 1, k)$$

is in general not an isomorphism.

Hasse invariant

- In Serre's theory, the modular form E_{p-1} plays a fundamental role:
$$E_{p-1} \equiv 1 \pmod{p}.$$
- In Katz's theory, this will be replaced by the Hasse invariant, which is a modular form in characteristic p.

Notation

- Let R be a ring in which $p = 0$, i.e. R is an $\mathbf{F}_p$-algebra.
- Consider $(E/R, \omega)$ where E is an elliptic curve over R and ω is a basis of $\underline{\omega}_{E/R} = H^0(E, \Omega^1_{E/R})$.
- By Serre duality, $\omega \in H^0(E, \Omega^1_{E/R})$ determines a dual basis

$$\eta \in H^1(E, \mathcal{O}_E).$$

- Consider the absolute Frobenius

$$\begin{aligned} F_{\text{abs}} : \mathcal{O}_E &\to \mathcal{O}_E \\ f &\mapsto f^p. \end{aligned}$$

This induces $F_{\text{abs}}^* : H^1(E, \mathcal{O}_E) \to H^1(E, \mathcal{O}_E)$, which is $\mathbf{F}_p$-linear.

Hasse invariant

Definition (Hasse invariant)

Define $A(E/R, \omega) \in R$ by setting

$$F_{\mathrm{abs}}^*(\eta) = A(E/R, \omega)\eta$$

in $H^1(E, \mathcal{O}_E)$.

Remark

Passing to the dual $H^1(E, \mathcal{O}_E)$ allows us to see more structure; indeed, the absolute Frobenius kills $H^0(E, \Omega^1_{E/R})$:

$$F_{\mathrm{abs}}^*(dx) = d(x^p) = 0.$$

Equivalently, we can study the Verschiebung operator V on $H^0(E, \Omega^1_{E/R})$.

Hasse invariant and supersingular elliptic curves

Remark

- Suppose R is a field with $\mathrm{char}(R) = p$. Then E is supersingular if and only if $A(E, \omega) = 0$ for any choice of ω.
- Over $\mathbf{F}_p$, the key relation is

$$\#E(\mathbf{F}_p) = 1 + p - \mathrm{tr}\left(F_{\mathrm{abs}}^* : H^1(E, \mathcal{O}_E) \to H^1(E, \mathcal{O}_E)\right).$$

Note that F_{abs}^* is multiplication by $A(E, \omega)$, so its trace equals $A(E, \omega)$ in $\mathbf{F}_p$ and

$$\#E(\mathbf{F}_p) \equiv 1 \pmod{p} \iff A(E, \omega) = 0.$$

Hasse invariant as a modular form

Lemma

$A(E/R, \omega) \in M(\mathbf{F}_p; 1, p-1)$ is a (meromorphic) modular form of weight $p-1$.

Proof.

If ω is scaled by λ, then η is scaled by λ^{-1}. Then

$$\begin{aligned} A(E, \lambda\omega)(\lambda^{-1}\eta) &= F^*_{\mathrm{abs}}(\lambda^{-1}\eta) \\ &= \lambda^{-p} F^*_{\mathrm{abs}}(\eta) \\ &= \lambda^{-p} A(E, \omega)\eta \end{aligned}$$

and hence $A(E, \lambda\omega) = \lambda^{1-p} A(E, \omega)$. □

Hasse invariant: q-expansion

Question

What is its q-expansion?

Katz gives two approaches:

1. dualizing sheaf;
2. derivations.

Sketch of second approach:

- $H^1(E, \mathcal{O}_{E/R}) = \mathrm{Lie}_R(E)$ can be identified as the R-module of invariant derivations of E.
- In general, iterating a derivation does not yield a derivation, but in characteristic p we have

$$D^p(xy) = \sum_{i=0}^{p} \binom{p}{i} (D^i x)(D^{p-i} y) = (D^p x)y + x(D^p y)$$

so D^p is a derivation.

Hasse invariant: q-expansion

- $F_{\mathrm{abs}}^* : H^1(E, \mathcal{O}_E) \to H^1(E, \mathcal{O}_E)$ is given by $D \mapsto D^p$.
- To compute the q-expansion of A, consider $(\mathrm{Tate}(q), \omega_{\mathrm{can}})$ and the derivation D dual to ω_{can}, so that

$$A(\mathrm{Tate}(q), \omega_{\mathrm{can}})D = D^p.$$

- Interpret $(\mathrm{Tate}(q), \omega_{\mathrm{can}})$ as $\left(\mathbf{G}_m/q^{\mathbf{Z}}, \frac{du}{u}\right)$.
- For the formal parameter t of $\mathrm{Tate}(q)$ at identity, $\omega_{\mathrm{can}} = \frac{dt}{1+t}$.
- The dual derivation is given by $D(t) = 1 + t$, so that

$$D(1+t) = 1 + t \implies D^n(1+t) = 1 + t \text{ for all } n \geq 1.$$

- Hence $D^p = D$ and $A(\mathrm{Tate}(q), \omega_{\mathrm{can}}) = 1$.

Hasse invariant: q-expansion

Therefore we have shown

Theorem

$A \in S(\mathbf{F}_p; 1, p-1)$ is a holomorphic modular form of weight $p-1$, with q-expansion 1.

Remark

- This works for all p, including $p = 2$ and $p = 3$! In particular,

$$S(\mathbf{Z}; 1, p-1) \otimes_{\mathbf{Z}} \mathbf{F}_p \to S(\mathbf{F}_p; 1, p-1)$$

  fails to be an isomorphism for $p = 2, 3$: the source is 0 but the target contains A.
- Note that $1 \notin S(\mathbf{F}_p; 1, p-1)$, so this theorem doesn't violate the q-expansion principle.

Lifting the Hasse invariant

- Recall the weight k Eisenstein series for even $k \geq 4$:

$$E_k = 1 - \frac{2k}{B_{2k}} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n.$$

  By the q-expansion principle, $E_k \in S(\mathbf{Q}; 1, k)$.

- For $k = p - 1$ and $p \geq 5$, $v_p\left(\frac{2(p-1)}{B_{2(p-1)}}\right) = 1$, so reduction mod p gives

$$\overline{E}_{p-1} \in S(\mathbf{F}_p; 1, p-1)$$

  with q-expansion 1.

- By the q-expansion principle again,

$$A \equiv E_{p-1} \pmod{p}.$$

- In other words, E_{p-1} is a lift of A to $\mathbf{Z}$ if $p \geq 5$.

Lifting the Hasse invariant

- If $p = 2$ (resp. $p = 3$), A does not lift to a holomorphic modular form of level 1, but E_4 is a lift of A^4 (resp. of A^2).
- To define p-adic modular forms, we need to fix a lift of A itself (of possibly higher level). A careful study of base-change shows:

Proposition

A lifts to a holomorphic modular form in $S\left(\mathbf{Z}[\frac{1}{N}]; N, p-1\right)$ when:

- $p = 2$*:* $N = 3, 5, 7, 9, 11$ *(hence any multiples of these);*
- $p = 3$*:* $N \geq 2$ *with* $3 \nmid N$*;*
- $p \geq 5$*:* $N \geq 1$ *with* $5 \nmid N$*.*

From now on, we restrict to these settings and fix a choice of lift $E_{p-1} \in S\left(\mathbf{Z}[\frac{1}{N}]; N, p-1\right)$ (by an abuse of notation).

Motivations

- To develop a p-adic theory of modular forms, taking $S(R; N, k)$ for a p-adic coefficient ring R is too simplistic: it is essentially the base-change of $S(\mathbf{Z}[\frac{1}{N}]; N, k)$ and does not incorporate the p-adic topology.
- For example, $E_{p-1} \equiv 1 \pmod{p}$ implies $E_{p-1}^{p^m} \to 1$ p-adically, so

$$E_{p-1}^{-1} = \lim_{m\to\infty} E_{p-1}^{p^m-1}$$

should exist.
- On the other hand, if E is a supersingular elliptic curve, then $E_{p-1}(E/R, \omega) = 0$.

Idea

Remove the elliptic curves which are supersingular (or have supersingular reduction) in the modular definition of p-adic modular forms.

Notation

- (p, N): such that $A \in S(\mathbf{F}_p; 1, p-1)$ has a lift $E_{p-1} \in S(\mathbf{Z}[\frac{1}{N}]; N, p-1)$ (simplest case: $p \geq 5$)
- R_0: a p-adically complete ring, i.e. $R_0 = \varprojlim R_0/p^m R_0$
- r: a fixed element of R_0 ("growth condition")

Idea

Remove the test objects which are not "too supersingular", i.e. whose Hasse invariant lies in a disk of radius $|r|_p$ around 0:

- $|r| = 1$: ordinary locus
- $|r| < 1$: a "thickening" of the ordinary locus

r-test objects

Definition

An r-**test object** is $(E/R, \omega, \alpha_N, Y)$ where:

- E is an elliptic curve over an R_0-algebra R in which p is nilpotent (i.e. $p^m = 0$ for some m);
- ω is basis of $\underline{\omega}_{E/R}$;
- α_N is a level N structure;
- $Y \in R$ with $E_{p-1}(E/R, \omega, \alpha_N) \cdot Y = r$.

Remark

The base ring R_0 is p-adically complete, but p is nilpotent in the test ring R.

p-adic modular forms with growth conditions

Definition

A ***p*-adic modular form over R_0 of growth r, level N and weight k** is a rule f that assigns

$$r\text{-test object } (E/R, \omega, \alpha_N, Y) \mapsto f(E/R, \omega, \alpha_N, Y) \in R$$

which:

- depends only on the R-isomorphism class of the r-test object;
- commutes with base change;
- satisfies

$$f(E/R, \lambda\omega, \alpha_N, \lambda^{p-1}Y) = \lambda^{-k} f(E/R, \omega, \alpha_N, Y)$$

  for $\lambda \in R^\times$.

The R-module of such is denoted $M(R_0; r, N, k)$.

p-adic modular forms with growth conditions

Remark

- Reality check: $(E/R, \lambda\omega, \alpha_N, \lambda^{p-1}Y)$ remains an r-test object:

$$r = E_{p-1}(E/R, \omega, \alpha_N) \cdot Y = E_{p-1}(E/R, \lambda\omega, \alpha_N) \cdot \lambda^{p-1} Y.$$

- As usual, it is equivalent to consider rules

$$(E/S, \alpha_N, Y) \mapsto f(E/S, \alpha_N, Y) \in H^0(S, \underline{\omega}_{E/S}^{\otimes k})$$

where:

  - S is any R_0-scheme with p nilpotent;
  - Y is a section of $\underline{\omega}_{E/S}^{\otimes(1-p)}$ with $Y \cdot E_{p-1}(E/S, \alpha_N) = r$;

satisfying the expected conditions.

Growth conditions

Growth condition r:

- The growth condition only depends on $r \cdot R_0^\times$, i.e. on $|r|_p$.
- Choosing $|r| = 1$ (i.e. $r \in R_0^\times$ is a unit) gives a "convergent" p-adic modular form, in the sense of being convergent on the ordinary locus.
- Choosing $|r| < 1$ (i.e. $p^\alpha \mid r$ for some $\alpha > 0$) gives an overconvergent p-adic modular form, in the sense of being convergent **beyond** the ordinary locus. Indeed, some of the test objects might have supersingular reduction.
- Why? The space of (convergent) p-adic modular forms is too large, but the overconvergent modular forms enjoy better properties; we will see instances of this next time.

p-adic modular forms

- We say that $f \in M(R_0; r, N, k)$ is holomorphic at ∞ if for every integer $m \geq 1$ and every level N structure α_N,

$$f\left(\mathrm{Tate}(q^N), \omega_{\mathrm{can}}, \alpha_N, r \cdot E_{p-1}(\mathrm{Tate}(q^N), \omega_{\mathrm{can}})^{-1}\right) \in \mathbf{Z}((q)) \otimes (R_0/p^m R_0)[\zeta_N]$$

  belongs to $\mathbf{Z}[[q]] \otimes (R_0/p^m R_0)[\zeta_N]$.
- The space of holomorphic forms is denoted $S(R_0; r, N, k)$.
- Formally

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

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

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

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