p-adic modular forms

TCC (Spring 2021), Lecture 3

Pak-Hin Lee

4th February 2021

Administrative issues

Slides:

- Lectures 1 and 2 available on webpage

Problem sheets:

- 3 sets for assessment
  1. 19th February (Friday of Week 5)
  2. 5th March (Friday of Week 7)
  3. 19th March (Friday of Week 9)
- available two weeks before deadlines

Emails:

- Thank you all for your introductory email!
- Still working through responses...

Recap: Congruences between modular forms

- (Swinnerton-Dyer) Structure of mod p modular forms:

$$f \equiv f' \pmod{p} \implies k \equiv k' \pmod{p-1}.$$

- (Serre) Refinement for higher congruences:

Theorem (théorème 1, P.198 of Antwerp)

Suppose $f \in M_{k,\mathbf{Q}}$ and $f' \in M_{k',\mathbf{Q}}$ satisfy $f \neq 0$ and

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

for some $m \geq 1$. Then

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

Recap: Filtration degree

Recall that $\widetilde{E}_{p-1} = 1$ gives

$$\widetilde{M}_k \subset \widetilde{M}_{k+p-1} \subset \widetilde{M}_{k+2(p-1)} \subset \cdots .$$

Definition (Filtration degree)

For $\widetilde{f} \in \widetilde{M}$,

$$w(\widetilde{f}) := \begin{cases} \min\{k \in \mathbf{Z}_{\geq 0} : \widetilde{f} \in \widetilde{M}_k\} & \text{if } \widetilde{f} \neq 0, \\ -\infty & \text{if } \widetilde{f} = 0. \end{cases}$$

Recap: Filtration degree

Proposition

Let $f \in M_{k,\mathbf{Z}_{(p)}}$ *with* $\widetilde{f} \neq 0$. *Then:*

1. $w(\widetilde{f}) < k$ *if and only if* $\widetilde{A}$ *divides* $\widetilde{\Phi}$, *where* $\Phi \in \mathbf{Z}_{(p)}[X, Y]$ *is such that* $f = \Phi(Q, R)$.
2. $w(\Theta\widetilde{f}) \leq w(\widetilde{f}) + p + 1$, *with equality if and only if* $w(\widetilde{f}) \not\equiv 0 \pmod{p}$.
3. $w(\widetilde{f}^i) = iw(\widetilde{f})$.

Game plan

- Finish the proof of main theorem (théorème 1) concerning higher congruences between classical modular forms
- Basic ingredients:
  1. structure of mod p modular forms
  2. Clausen–von Staudt theorem
- New ingredients:
  1. filtration on $\widetilde{M}$: introduced in both Swinnerton-Dyer [Antwerp] and Serre [Bourbaki]
  2. geometry of $\widetilde{M}$: presented in Serre [Bourbaki] only
- I will try to motivate each step and explain some details omitted by Serre [Antwerp].

Reduction of main theorem

Recall: By suitably scaling f and replacing f' with $f' E_{p^{n-1}(p-1)}$, we have reduced the main theorem (théorème 1) to:

Theorem

Let $p \geq 5$. Suppose $f \in M_{k,\mathbf{Z}_{(p)}}$ and $f' \in M_{k',\mathbf{Z}_{(p)}}$ satisfy:

- $v_p(f) = 0$;
- $f \equiv f' \pmod{p^m}$ *for* $m \geq 2$;
- $h := k' - k \geq 4$ *(known: $h \equiv 0 \pmod{p-1}$).*

Then

$$r := v_p(h) + 1 \geq m.$$

Proof of main theorem

Suppose for the sake of contradiction that $r < m$.

Idea

Match the weights of f and f'.

Consider the weight k' form

$$fE_h - f' = (f - f') + f(E_h - 1),$$

where

- $p^m \mid f - f'$ by hypothesis
- $p^r \mid\mid E_h - 1$ by:

Corollary (Clausen–von Staudt)

$E_k \equiv 1 \pmod{p^n} \iff p^{n-1}(p-1) \mid k.$

Proof of main theorem

- $r < m$ implies

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

Idea

Focus on $E_h - 1$, which has an explicit q-expansion.

- Write $p^{-r}(E_h - 1) = \lambda\phi$ where $\phi = \sum_{n\geq 1}\sigma_{h-1}(n)q^n$ and $v_p(\lambda) = 0$.
- Then

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

- Set $g := \lambda^{-1}p^{-r}(fE_h - f')$, so that

$$g \equiv f\phi \pmod{p}.$$

Proof of main theorem

- Now $\phi = \sum_{n\geq 1} \sigma_{h-1}(n) q^n$ satisfies

$$\widetilde{g} = \widetilde{f}\widetilde{\phi}$$

  for some $g \in M_{k',\mathbf{Z}_{(p)}}$, $f \in M_{k,\mathbf{Z}_{(p)}}$.
- Since $k \equiv k' \pmod{p-1}$, this shows

$$\widetilde{\phi} \in \operatorname{Frac} \widetilde{M}^0.$$

Theorem

$\widetilde{M}^0$ is a Dedekind domain.

See Serre [Bourbaki]: Spec $\widetilde{M}^0 = \mathbf{P}^1_{j,\mathbf{F}_p} - \{\text{ss points}\}$ is a smooth affine curve. (Question: Is there an "algebraic" proof?)

Proof of main theorem

Idea

Show that $\widetilde{\phi}$ is integral over $\widetilde{M}^0$ ($\implies \widetilde{\phi} \in \widetilde{M}^0$).

Consider

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

Lemma

1. $\phi - \phi^p \equiv \psi \pmod{p}$.
2. $\psi \equiv -\frac{1}{24} \Theta^{p-2}(E_{p+1}) \pmod{p}$. *In particular,* $\widetilde{\psi} \in \widetilde{M}^0$.

Let me fill in the details, which are omitted by Serre [Antwerp].

Proof of identity (1): extracting the prime-to-p terms

- Raising $\phi = \sum_{n \geq 1} \sigma_{h-1}(n) q^n$ to the p-th power gives

$$\begin{aligned} \phi^p &\equiv \sum_{n \geq 1} \sigma_{h-1}(n) q^{pn} \pmod{p} \quad \text{[Fermat's little theorem]} \\ &\equiv \sum_{n \geq 1} \sigma_{h-1}(pn) q^{pn} \pmod{p} \\ &\equiv \sum_{p \mid n} \sigma_{h-1}(n) q^n \pmod{p}. \end{aligned}$$

- Hence

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

for

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

Proof of identity (2): relating with E_2

If $(n, p) = 1$, then Fermat's little theorem with $(p-1) \mid h$ implies

$$\sigma_{h-1}(n) = \sum_{d|n} d^{h-1} \equiv \sum_{d|n} d^{-1} = \sum_{d|n} \frac{nd^{-1}}{n} = \frac{\sigma_1(n)}{n} \pmod{p}.$$

Thus

$$\begin{aligned}
\psi &= \sum_{(n,p)=1} \sigma_{h-1}(n) q^n \\
&\equiv \sum_{(n,p)=1} \frac{\sigma_1(n)}{n} q^n \pmod{p} \\
&\equiv \sum_{n=1}^{\infty} n^{p-2} \sigma_1(n) q^n \pmod{p} \\
&\equiv \Theta^{p-2} \left(\sum_{n=1}^{\infty} \sigma_1(n) q^n \right) \pmod{p}.
\end{aligned}$$

Proof of identity (2): relating with E_{p+1}

Recall $E_2 = 1 - 24\sum_{n\geq 1}\sigma_1(n)q^n$. Hence

$$\begin{aligned}\psi &\equiv -\frac{1}{24}\Theta^{p-2}(E_2) \pmod p\\ &\equiv -\frac{1}{24}\Theta^{p-2}(E_{p+1}) \pmod p.\end{aligned}$$

Recall $\Theta : \widetilde{M}_k \to \widetilde{M}_{k+p+1}$ (note: $k+p+1$ might not be the optimal weight $w(\Theta\widetilde{f})$, but this doesn't matter for now), so

$$\widetilde{\psi} = -\frac{1}{24}\Theta^{p-2}(\widetilde{E}_{p+1})$$

belongs to $\widetilde{M}_{(p+1)+(p+1)(p-2)} = \widetilde{M}_{(p+1)(p-1)} \subset \widetilde{M}^0$.

Proof of main theorem

Summary so far:

- $\widetilde{\phi} - \widetilde{\phi}^p = \widetilde{\psi}$.
- $\widetilde{\phi} \in \operatorname{Frac} \widetilde{M}^0$.
- $\widetilde{\psi} \in \widetilde{M}^0$.

Since $\widetilde{M}^0$ is a Dedekind domain, hence integrally closed, we conclude

$$\widetilde{\phi} \in \widetilde{M}^0.$$

Proof of main theorem: filtration degrees

Take filtration degrees on both sides of

$$\widetilde{\phi} - \widetilde{\phi}^p = -\frac{1}{24}\Theta^{p-2}(\widetilde{E}_{p+1}).$$

LHS:

- $w(\widetilde{\phi}^p) = pw(\widetilde{\phi})$.
- Write $\widetilde{\phi} = \Phi(\widetilde{Q}, \widetilde{R})$ where $\widetilde{A} \nmid \Phi$. Then $\widetilde{\phi} - \widetilde{\phi}^p$ can be represented by a homogeneous polynomial of the form $\Phi\widetilde{A}^n - \Phi^p$, which is not divisible by $\widetilde{A}$.
- Hence $w(\mathrm{LHS}) = pw(\widetilde{\phi})$.

RHS:

- $w(\mathrm{RHS}) \leq (p+1) + (p+1)(p-2) = (p+1)(p-1)$.
- Equality holds because $(p+1) + (p+1)i$ is never divisible by p for $i = 0, 1, \cdots, p-2$.

Proof of main theorem: contradiction!

We have shown

$$pw(\widetilde{\phi}) = (p+1)(p-1)$$

which is a contradiction!

Remark

The equation $\widetilde{\phi} - \widetilde{\phi}^p = \widetilde{\psi}$ defines an (irreducible) degree p cover of Spec $\widetilde{M}^0 = X_0(1)^{\mathrm{ord}}_{\mathbf{F}_p}$.

Overview of Serre's theory

- Classical modular forms exhibit natural p-adic properties:

$$f \text{ and } f' \text{ ``}p\text{-adically close''} \implies k \text{ and } k' \text{ ``}p\text{-adically close''}.$$

- Serre's idea:

$$p\text{-adic modular forms} = \begin{array}{l}\text{``}p\text{-adic limits'' of } q\text{-expansions} \\ \text{of classical modular forms.}\end{array}$$

- This is elementary – as opposed to Katz's algebro-geometric theory – but already quite powerful.

Motivation: p-adic zeta functions

- Special values of the Riemann zeta function: $\zeta(1-k) = -\frac{B_k}{k}$ at the negative odd integers
- Kummer congruence: If k, k' are even integers not divisible by $p-1$ with $k \equiv k' \pmod{p^m(p-1)}$, then

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

- Roughly speaking, $(1-p^{-s})\zeta(s)$ (with Euler factor at p removed) is p-adically continuous.
- Leopoldt–Kubota: construction of the p-adic zeta function interpolating these values
- Serre: alternative construction as the constant term of p-adic Eisenstein series
- **Slogan:** the non-constant Fourier coefficients govern the constant term.

Motivation: congruences of modular forms

- Classical theory: combinatorial arguments for congruences such as

$$\tau(n) \equiv \sigma_{11}(n) \pmod{691}$$

  for $\Delta = \sum_{n=1}^{\infty} \tau(n) q^n$ (Ramanujan, 1916).

- Mod p theory: Problem Sheet 1 will ask you to show

$$\tau(n) \equiv n\sigma_5(n) \pmod{5},$$
$$\tau(n) \equiv n\sigma_3(n) \pmod{7}.$$

  See Swinnerton-Dyer [Antwerp] and Serre [Bourbaki] for many others.

Motivation: congruences of modular forms

- p-adic theory: provides conceptual framework for understanding congruences such as

$$\begin{aligned} c(2^a n) &\equiv 0 \pmod{2^{3a+8}}, \\ c(3^a n) &\equiv 0 \pmod{3^{2a+3}}, \\ c(5^a n) &\equiv 0 \pmod{5^{a+1}}, \\ c(7^a n) &\equiv 0 \pmod{7^a}, \\ c(11^a n) &\equiv 0 \pmod{11^a} \end{aligned}$$

for the j-invariant $j(\tau) = \sum_{n=-1}^{\infty} c(n)q^n$ (Lehner, 1949; Atkin, 1966 – via intricate manipulations).

Remark

J. Lehner $\neq$ D.H. Lehmer; both have worked on modular forms!

- **Slogan:** contraction property of U_p-operator

Notation

Consider the p-adic numbers $\mathbf{Q}_p$, with

- valuation $v_p : \mathbf{Q}_p \to \mathbf{Z} \cup \{\infty\}$ given by $v_p(p) = 1$;
- absolute value $|\cdot|_p : \mathbf{Q}_p \to \mathbf{Q}_{\geq 0}$ given by $|x|_p = p^{-v_p(x)}$.

Extend the p-adic valuation to $v_p : \mathbf{Q}_p[[q]] \to \mathbf{Z} \cup \{\pm\infty\}$ by

$$f = \sum_{n=0}^{\infty} a_n q^n \mapsto v_p(f) := \inf_{n \geq 0} v_p(a_n).$$

f has bounded coefficients $\iff f \in \mathbf{Z}_p[[q]] \otimes \mathbf{Q}_p \iff v_p(f) > -\infty$; this includes all $f \in M_{k,\mathbf{Q}}$.

Remark

$\mathbf{Z}_p[[q]] \otimes \mathbf{Q}_p$ is a p-adic Banach space with $|f| := \sup_{n \geq 0} |a_n|_p$.

Notation

- $v_p(f) \geq 0$ means $f \in \mathbf{Z}_p[[q]]$, i.e. f has p-integral coefficients.
- If $v_p(f) \geq m$, we write

$$f \equiv 0 \pmod{p^m}.$$

- If (f_i) is a sequence of elements in $\mathbf{Q}_p[[q]]$, we say $f_i \to f$ if $v_p(f - f_i) \to \infty$, i.e. the coefficients of f_i tend to those of f **uniformly**.

Convergence in $\mathbf{Q}_p[[q]]$

$$
\begin{aligned}
f_1 &= a_0^{(1)} + a_1^{(1)} q + \cdots + a_n^{(1)} q^n + \cdots , \\
f_2 &= a_0^{(2)} + a_1^{(2)} q + \cdots + a_n^{(2)} q^n + \cdots , \\
&\vdots \\
f_i &= a_0^{(i)} + a_1^{(i)} q + \cdots + a_n^{(i)} q^n + \cdots , \\
&\vdots \\
f &= a_0 + a_1 q + \cdots + a_n q^n + \cdots
\end{aligned}
$$

$f_i \to f$ means $a_n^{(i)} \to a_n$ uniformly in n.

p-adic modular forms

Definition (Serre)

A **p-adic modular form** is a formal power series $f \in \mathbf{Q}_p[[q]]$ such that there exists a sequence of modular forms $f_i \in M_{k_i,\mathbf{Q}}$ of weight k_i such that

$$f_i \to f.$$

Denote by $M^\dagger \subset \mathbf{Q}_p[[q]]$ (in fact, $\subset \mathbf{Z}_p[[q]] \otimes \mathbf{Q}_p$) the space of p-adic modular forms.

At first glance, the sequence f_i might seem arbitrary. Recall théorème 1 (on congruences mod p^m) imposes strong conditions on the behavior of (k_i) – this is remarkable!

Weights

Theorem (théorème 1)

Suppose $f \in M_{k,\mathbf{Q}}$ *and* $f' \in M_{k',\mathbf{Q}}$ *satisfy* $f \neq 0$ *and*

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

for some $m \geq 1$. *Then*

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

This suggests looking at the inverse limit of $\mathbf{Z}/\left(p^{m-1}(p-1)\right)\mathbf{Z}$ (resp. $\mathbf{Z}/2^{m-2}\mathbf{Z}$).

Weight space

Definition (Weight space)

For $m \geq 1$, set

$$\mathfrak{X}_m := \begin{cases} \mathbf{Z}/\left(p^{m-1}(p-1)\right)\mathbf{Z} & \text{if } p \neq 2, \\ \mathbf{Z}/2^{m-2}\mathbf{Z} & \text{if } p = 2, \end{cases}$$

and

$$\mathfrak{X} := \varprojlim_m \mathfrak{X}_m = \begin{cases} \mathbf{Z}_p \times \mathbf{Z}/(p-1)\mathbf{Z} & \text{if } p \neq 2, \\ \mathbf{Z}_2 & \text{if } p = 2. \end{cases}$$

Remark

The natural projection maps $\mathbf{Z} \to \mathfrak{X}_m$ induce an injection $\mathbf{Z} \to \mathfrak{X}$ with dense image.

Weights as characters of $\mathbf{Z}_p^\times$

$\mathfrak{X} = \mathbf{Z}_p \times \mathbf{Z}/(p-1)\mathbf{Z}$ (resp. $\mathbf{Z}_2$) can be identified as the group of continuous characters $\mathbf{Z}_p^\times \to \mathbf{C}_p^\times$.

- Suppose $p \geq 3$. Then $\mathbf{Z}_p^\times \cong (1 + p\mathbf{Z}_p) \times \mu_{p-1}$.
- $1 + p\mathbf{Z}_p$ is isomorphic to the additive group of $\mathbf{Z}_p$ (via p-adic logarithm); its continuous characters are given by $\gamma \mapsto \gamma^s$ for any $s \in \mathbf{Z}_p$.
- μ_{p-1} is the group of $(p-1)$-st roots of unity (via Teichmüller character); its characters are given by $\zeta \mapsto \zeta^u$ for any $u \in \mathbf{Z}/(p-1)\mathbf{Z}$.
- Hence, the continuous characters of $\mathbf{Z}_p^\times$ are given by pairs $k = (s, u) \in \mathbf{Z}_p \times \mathbf{Z}/(p-1)\mathbf{Z}$ sending

$$x = (\gamma, \zeta) \mapsto x^k := (\gamma^s, \zeta^u).$$

Weights as characters of $\mathbf{Z}_p^\times$

- The (dense) image of $\mathbf{Z} \to \mathfrak{X}$ corresponds to characters $x \mapsto x^k$ for $k \in \mathbf{Z}$, also called the **integral weights**.
- The case for $p = 2$ can be analyzed similarly.

Definition

We say that $k \in \mathfrak{X}$ is **even** if $k \in 2\mathfrak{X}$, or equivalently $(-1)^k = 1$.

When $p \neq 2$, this means $k = (s, u) \in \mathbf{Z}_p \times \mathbf{Z}/(p-1)\mathbf{Z}$ with u even (and s arbitrary – it is always possible to divide by 2 in $\mathbf{Z}_p$).

Convergence of weights in $\mathfrak{X}$

Theorem

Let $f \neq 0$ be a p-adic modular form, and $f_i \in M_{k_i,\mathbf{Q}}$ be a sequence with $f_i \to f$. Then:

1. *k_i converges to some $k \in \mathfrak{X} = \varprojlim_m \mathfrak{X}_m$.*
2. *The limit k depends only on f but not the choice of the sequence (f_i).*

- By convergence $f_i \to f$ (uniformly in n), we have

$$v_p(f_i) = v_p(f)$$

  for $i \gg 0$.
- This is in $\mathbf{Z}$ (and not ∞) since $f \neq 0$.

Convergence of weights in $\mathfrak{X}$

- For each $m \geq 1$, we have for $j \geq i \gg 0$

$$v_p(f_j - f_i) \geq v_p(f) + m = v_p(f_i) + m.$$

- By Serre's théorème 1,

$$k_i \equiv k_j \pmod{p^{m-1}(p-1)}$$

  for all sufficiently large i and j, i.e. $k_i \in \mathfrak{X}_m$ is stationary in i.
- Therefore $k = \lim k_i \in \mathfrak{X}$ exists.
- To prove (2): If (f_i') is another sequence with $f_i' \to f$, consider the new sequence

$$f_1, f_1', f_2, f_2', \cdots, f_i, f_i', \cdots.$$

Weights of p-adic modular forms

Definition

We call $k \in \mathfrak{X}$ the **weight** of the p-adic modular form f, and denote by $M_k^\dagger$ the space of p-adic modular forms of weight k.

- k is in general not an integer ($\in \mathbf{Z}$) – not even a p-adic integer ($\in \mathbf{Z}_p$)!
- $k \in \mathfrak{X}$ is necessarily even, being a limit of even weights $k_i \in \mathbf{Z}$.
- $M_0^\dagger \subset M^\dagger$ is a subalgebra, and $M_k^\dagger$ is an $M_0^\dagger$-module.

Examples

Example (Trivial)

Since $E_{p-1} \equiv 1 \pmod{p}$,

$$E_{p-1}^{p^m} \equiv 1 \pmod{p^{m+1}}.$$

Thus $E_{p-1}^{p^m} \in M_{(p-1)p^m,\mathbf{Q}}$ with limit 1, so 1 is a p-adic modular form of weight $\lim (p-1)p^m = 0 \in \mathfrak{X}$.

Example

The same argument shows

$$\frac{1}{E_{p-1}} = \lim E_{p-1}^{p^m - 1}$$

is a p-adic modular form of weight $\lim (p-1)(p^m - 1) = 1 - p$.

Examples

Example

For $p = 5$ and $Q = E_4$, this shows

$$\frac{1}{Q} \in M^{\dagger}_{-4} \quad \text{and} \quad \frac{1}{j} = \frac{\Delta}{Q^3} \in M^{\dagger}_{0}.$$

Problem Sheet 1:

$$M_0^{\dagger} = \mathbf{Q}_5 \left\langle \frac{1}{j} \right\rangle$$

where $\mathbf{Q}_p\langle T\rangle = \{\sum_{n=0}^{\infty} c_n T^n : c_n \in \mathbf{Q}_p, v_p(c_n) \to \infty\}$ is the Tate algebra.

Properties of p-adic modular forms

Our previous results on congruences and convergence carry over to p-adic modular forms, by a basic limiting argument:

Theorem

1. *Suppose* $f \in M_k^\dagger$ *and* $f' \in M_{k'}^\dagger$ *satisfy* $f \neq 0$ *and*

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

for some $m \geq 1$. *Then* k *and* k' *have the same image in* $\mathfrak{X}_m$.

2. *If* $f_i \in M_{k_i}^\dagger$ *is a sequence of p-adic modular forms of weight* $k_i \in \mathfrak{X}$ *with* $f_i \to f \in \mathbf{Q}_p[[q]]$, *then* f *is a p-adic modular form of weight* $k = \lim k_i$.

Thus $M^\dagger$ is a p-adic Banach space (as a closed subspace of $\mathbf{Z}_p[[q]] \otimes \mathbf{Q}_p$), equipped with a continuous map $M^\dagger \to \mathfrak{X}$ (weight map).