p-adic modular forms

TCC (Spring 2021), Lecture 2

Pak-Hin Lee

28th January 2021

Eisenstein series of weight 2

Recall the “fake” weight 2 Eisenstein series

$$P = E_2 := 1 - 24 \sum_{n=1}^{\infty} \sigma_1(n) q^n.$$

This is not a modular form: it is invariant under translation but transforms under inversion as

$$P\left(-\frac{1}{\tau}\right) = \tau^2 P(\tau) + \frac{12\tau}{2\pi i}.$$

Theta operator

Definition

The Ramanujan (or Atkin–Serre) theta operator is

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

- On q-expansions, $f = \sum a_n q^n$ is sent to $\Theta f = \sum n a_n q^n$.
- In complex coordinates, Θ is given by $\dfrac{1}{2\pi i}\dfrac{d}{d\tau}$, where $q = e^{2\pi i\tau}$.
- Although Θ does not preserve modularity, the discrepancy is a simple expression involving P.

Theta operator

Theorem (Ramanujan)

1. *If f is a modular form of weight k, then*

$$\Theta f - \frac{k}{12} P f$$

   is a modular form of weight $k+2$.

2. *Θ acts on P, Q, R by*

$$\Theta P = \frac{1}{12}(P^2 - Q),$$
$$\Theta Q = \frac{1}{3}(PQ - R),$$
$$\Theta R = \frac{1}{2}(PR - Q^2).$$

Theta operator

Corollary

$\mathbf{Z}_{(p)}[P, Q, R] \subset \mathbf{Z}_{(p)}[[q]]$ *is stable under* Θ.

These are straightforward; note that ΘP requires a separate calculation!

Example

For $k = 12$,

$$\Theta\Delta - P\Delta \in M_{14}$$

which is one-dimensional and spanned by E_{14}. But its constant term is 0, so

$$\Theta\Delta - P\Delta = 0,$$

i.e. P is the logarithmic derivative of Δ.

Theta operator on mod p modular forms

Next we pass to mod p modular forms.
Although Θ fails to preserve modularity in the classical setting, the miracle is that it preserves the space of mod p modular forms!
First we recall some further facts about Bernoulli numbers.

Bernoulli numbers

Theorem

1. *(Clausen–von Staudt) If* $(p-1) \mid k$, *then* $v_p(B_k) = -1$.
2. *(Kummer) If* $(p-1) \nmid k$, *then* $\frac{B_k}{k} \in \mathbf{Z}_{(p)}$ *and*

$$\frac{B_k}{k} \equiv \frac{B_{k'}}{k'} \pmod{p} \quad \text{whenever } k \equiv k' \not\equiv 0 \pmod{p-1}.$$

Corollary

1. $E_{p-1} \in M_{p-1,\mathbf{Z}_{(p)}}$ *with* $\widetilde{E}_{p-1} = 1$.
2. $E_{p+1} \in M_{p+1,\mathbf{Z}_{(p)}}$ *with* $\widetilde{E}_{p+1} = \widetilde{P}$. *In particular,* $\widetilde{P} \in \widetilde{M}$ *is a mod p modular form.*

Bernoulli numbers

Proof.

We have already seen (1). For (2), we compare

$$E_{p+1} = 1 - \frac{2(p+1)}{B_{p+1}} \sum \sigma_p(n) q^n,$$
$$E_2 = 1 - \frac{4}{B_2} \sum \sigma_1(n) q^n.$$

Kummer's congruence gives $\frac{B_{p+1}}{p+1} \equiv \frac{B_2}{2} \equiv \frac{1}{12} \pmod{p}$ which is invertible (note: there is a typo in Equation (16) of Swinnerton-Dyer), while Fermat's little theorem gives $\sigma_p(n) \equiv \sigma_1(n) \pmod{p}$. Hence

$$E_{p+1} \equiv E_2 \pmod{p}.$$

□

Theta operator on mod p modular forms

Corollary

The algebra $\widetilde{M}$ of mod p modular forms is stable under Θ.

Proof.

If $f \in \widetilde{M}_k$, then

$$12\Theta f = \partial f + k\widetilde{P} f = \widetilde{E}_{p-1}\partial f + k\widetilde{E}_{p+1} f$$

where both summands belong to $\widetilde{M}_{k+p+1}$. □

Θ will play an important role in the p-adic theory.

A digression

- In the classical setting, the Maass–Shimura operator

$$\delta_k := \frac{1}{2\pi i}\left(\frac{d}{d\tau} + \frac{k}{\tau - \overline{\tau}}\right)$$

  transforms *real-analytic* modular forms of weight k into *real-analytic* modular forms of weight $k+2$.
- We will see that the theta operator Θ takes *p-adic* modular forms of weight k to *p-adic* modular forms of weight $k+2$.
- Indeed, there is a deep connection between them: they coincide at CM points (Shimura, Katz, etc.).

Derivation ∂ on modular forms

For $k \geq 4$, set

$$\partial := 12\Theta - kP : M_k \to M_{k+2}.$$

Then $\Theta Q = \frac{1}{3}(PQ - R)$ and $\Theta R = \frac{1}{2}(PR - Q^2)$ give:

Corollary

∂ defines a derivation on $\mathbf{Z}_{(p)}[Q, R]$ with

$$\partial Q = -4R, \quad \partial R = -6Q^2.$$

The same formulae define a derivation on $\mathbf{Z}_{(p)}[X, Y]$, hence on $\mathbf{F}_p[X, Y]$, with

$$\partial X = -4Y, \quad \partial Y = -6X^2.$$

The polynomials A and B

We have defined $A \in \mathbf{Z}_{(p)}[X, Y]$ to be the (unique) polynomial such that

$$E_{p-1} = A[Q, R].$$

Similarly, define $B \in \mathbf{Z}_{(p)}[X, Y]$ such that

$$E_{p+1} = B[Q, R].$$

The derivation ∂ acts on their mod p reductions by:

Lemma

$\partial\widetilde{A} = \widetilde{B}$ and $\partial\widetilde{B} = -\widetilde{Q}\widetilde{A}$. Thus $\widetilde{A}$ and $\widetilde{B}$ satisfy the differential equation

$$(\partial^2 + \widetilde{Q})\Phi = 0.$$

Finish of proof

Finally, we are ready to finish the last step in the proof:

$$\widetilde{M} = \mathbf{F}_p[X, Y]/(\widetilde{A} - 1)$$

$$\Uparrow$$

$\widetilde{A} - 1$ is irreducible

$$\Uparrow$$

$\widetilde{A}$ has no repeated factors

Idea

Differential operators detect repeated factors, and ∂ has a particularly nice description in terms of $\widetilde{A}$ and $\widetilde{B}$.

Proof: $\widetilde{A}$ has no repeated factors

Proposition

$\widetilde{A}$ has no repeated factors in $\overline{\mathbf{F}_p}[X,Y]$, and $\widetilde{A}$ and $\widetilde{B}$ are relatively prime.

- Recall that A is homogeneous of weight $p-1$, where X and Y have weights 4 and 6 respectively.
- Over an algebraic closure $\overline{\mathbf{F}_p}$, the irreducible factors of $\widetilde{A}$ must be of the form X, Y or $X^3 - cY^2$.
- Note $c \neq 1$. Otherwise, $\widetilde{Q}^3 - \widetilde{R}^2 \in q\mathbf{F}_p[[q]]$ has no constant term, but $\widetilde{A}(\widetilde{Q},\widetilde{R}) = 1$.
- Recall ∂ acts by

$$\partial X = -4Y, \quad \partial Y = -6X^2$$

and

$$\partial \widetilde{A} = \widetilde{B}, \quad \partial \widetilde{B} = -X\widetilde{A}.$$

Proof: $\widetilde{A}$ has no repeated factors

Factors of the form $X^3 - cY^2$ (where $c \neq 1$):

- Suppose $\widetilde{A}$ is exactly divisible by $(X^3 - cY^2)^n$ for some $n \geq 2$.
- Since

$$\partial(X^3 - cY^2) = 12(c-1)X^2Y$$

  is prime to $X^3 - cY^2$ (using $c \neq 1$), $\partial\widetilde{A} = \widetilde{B}$ is exactly divisible by $(X^3 - cY^2)^{n-1}$.
- Applying ∂ once more, $\partial\widetilde{B} = -X\widetilde{A}$ is exactly divisible by $(X^3 - cY^2)^{n-2}$, which is a contradiction.

Factors of the form X or Y are treated similarly.
As a by-product, we see that every factor of $\widetilde{A}$ with multiplicity n (necessarily 1) appears with multiplicity $n-1$ (necessarily 0) in $\partial\widetilde{A} = \widetilde{B}$. Thus $\widetilde{A}$ and $\widetilde{B}$ are co-prime.

Grading on mod p modular forms

We have shown the $\mathbf{F}_p$-algebra of mod p modular forms is isomorphic to

$$\widetilde{M} \cong \mathbf{F}_p[X,Y]/(\widetilde{A}-1).$$

Since $\widetilde{A}$ is homogeneous of weight $p-1$, we deduce

Corollary

$\widetilde{M}$ has a natural grading with values in $\mathbf{Z}/(p-1)\mathbf{Z}$, i.e.

$$\widetilde{M} = \bigoplus_{a\in\mathbf{Z}/(p-1)\mathbf{Z}} \widetilde{M}^a$$

where $\widetilde{M}^a = \sum_{k\equiv a \mod p-1} \widetilde{M}_k$.

In particular, $\widetilde{M}^0$ is a subalgebra.

Examples

Denote $Y = \operatorname{Spec} \widetilde{M}$ and $Y^0 = \operatorname{Spec} \widetilde{M}^0$.

Example ($p = 11$)

- $E_{10} = QR$, so the polynomial A is just XY.
- $\widetilde{M} = \mathbf{F}_{11}[X, Y]/(XY - 1)$, so $Y = \mathbf{P}^1 - \{0, \infty\}$
- $\widetilde{M}^0 = \mathbf{F}_{11}[X^5, Y^5]/(X^5 Y^5 - 1)$, so $Y^0 = \mathbf{P}^1 - \{0, \infty\}$.

Example ($p = 13$)

- $E_{12} = \dfrac{1}{691}(441 Q^3 + 250 R^2)$.
- $\widetilde{M} = \mathbf{F}_{13}[X, Y]/(X^3 + 10 Y^2 - 11)$, so Y is (the affine part of) an elliptic curve.
- $\widetilde{M}^0 = \mathbf{F}_{13}[X^3]$, so $Y^0 = \mathbf{A}^1$.

Geometric interpretation

Very brief remarks (see Serre's Bourbaki notes):

- $Y = \operatorname{Spec} \widetilde{M}$ and $Y^0 = \operatorname{Spec} \widetilde{M}^0$ are smooth affine curves (i.e. $\widetilde{M}$ and $\widetilde{M}^0$ are Dedekind domains).
- $Y^0 = \mathbf{P}^1_{j,\mathbf{F}_p} - \{\widetilde{A} = 0\}$.
- More precisely, Y is the ordinary locus of $X_0(p)_{\mathbf{F}_p}$, and Y^0 is the ordinary locus of $X_0(1)_{\mathbf{F}_p}$ (genus 0).
- The natural projection $Y \to Y^0$ is a covering with Galois group $\mathbf{F}_p^\times/\{\pm 1\}$.

Towards p-adic modular forms

Plans for Serre's article:

- Today: main theorem (théorème 1 on P.198) concerning congruences mod p^m between classical modular forms
- The last step of the proof involves two ingredients:
    1. filtration on $\widetilde{M}$: introduced in both Swinnerton-Dyer's article and Serre's Bourbaki notes
    2. geometry of $\widetilde{M}$: only presented in Serre's Bourbaki notes
- Next lecture: p-adic modular forms a là Serre
    1. motivations: p-adic zeta functions, congruences of modular forms
    2. Serre's theory: readily follows from main theorem
    3. applications

Main theorem on congruences mod p^m

From the structure of mod p modular forms, we have

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

Idea

This can be refined for congruences mod p^m. **Slogan:** If f and f' are congruent mod a high power of p, then so are k and k' (in addition to being congruent mod $p-1$).

Extend the p-adic valuation $v_p : \mathbf{Q}_p \to \mathbf{Z} \cup \{\infty\}$ (with $v_p(p) = 1$) to $\mathbf{Q}_p[[q]] \to \mathbf{Z} \cup \{\pm\infty\}$ by

$$f = \sum a_n q^n \mapsto v_p(f) = \inf_n v_p(a_n).$$

If f has bounded coefficients (e.g. $f \in M_{k,\mathbf{Q}}$), then $v_p(f) > -\infty$.

Main theorem on congruences mod p^m

Theorem (théorème 1 on P.198)

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*

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

First reduction:

- Scaling f and f' by $p^{-v_p(f)}$, we may assume $v_p(f) = 0$.
- The condition becomes $f \equiv f' \pmod{p^m}$; in particular, both have p-integral coefficients.

Main theorem on congruences mod p^m

Theorem

Suppose $f \in M_{k,\mathbf{Z}_{(p)}}$ *and* $f' \in M_{k',\mathbf{Z}_{(p)}}$ *satisfy* $v_p(f) = 0$ *and*

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

Then

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

As usual, we will focus on the case $p \geq 5$.

- For $m = 1$, this follows from our previous result on the structure of mod p modular forms.
- For general m, this requires the notion of *filtration degree*.

Filtration degree

Definition

For $\widetilde{f} \in \widetilde{M}$ nonzero, define its *filtration degree*

$$w(\widetilde{f}) := \min\{k \in \mathbf{Z}_{\geq 0} : \widetilde{f} \in \widetilde{M}_k\}.$$

By convention, $w(0) = -\infty$.

Thus $w(\widetilde{f})$ is the smallest k such that there exists a classical form of weight k reducing to $\widetilde{f}$ mod p.

Idea

Filtration degree ($\in \mathbf{Z}$) refines the weight ($\in \mathbf{Z}/(p-1)\mathbf{Z}$) of mod p modular forms.

Filtration degree

Proposition

Let $f \in M_{k,\mathbf{Z}_{(p)}}$ *be such that* $f = \Phi(Q, R)$ *for some* $\Phi \in \mathbf{Z}_{(p)}[X, Y]$, *and suppose* $\widetilde{f} \neq 0$. *Then:*

1. $w(\widetilde{f}) < k$ *if and only if* $\widetilde{A}$ *divides* $\widetilde{\Phi}$.
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. $w(\widetilde{f}^i) = iw(\widetilde{f})$.

Remark

Later we will study the effect of Hecke operators on $w(\widetilde{f})$.

Filtration degree

(1) is clear, since $\widetilde{M} = \mathbf{F}_p[X, Y]/(\widetilde{A} - 1)$.
Now assume f has been chosen so that $k = w(\widetilde{f})$ (thus $\widetilde{A} \nmid \widetilde{\Phi}$).
To prove (2), recall that $12\Theta = \partial + kP$, so

$$\begin{aligned} 12\Theta\widetilde{f} &= \partial\widetilde{f} + k\widetilde{P}\widetilde{f} = \widetilde{E}_{p-1}\partial\widetilde{f} + k\widetilde{E}_{p+1}\widetilde{f} \\ &= \widetilde{A}(\widetilde{Q}, \widetilde{R})\partial\widetilde{\Phi}(\widetilde{Q}, \widetilde{R}) + k\widetilde{B}(\widetilde{Q}, \widetilde{R})\widetilde{\Phi}(\widetilde{Q}, \widetilde{R}). \end{aligned}$$

Both $E_{p-1}\partial f$ and $E_{p+1}f$ belong to $M_{k+p+1,\mathbf{Z}_{(p)}}$, so

$$w(\Theta\widetilde{f}) \leq k + p + 1.$$

By (1), equality $\iff \widetilde{A} \nmid \widetilde{A}\partial\widetilde{\Phi} + k\widetilde{B}\widetilde{\Phi} \iff \widetilde{A} \nmid k\widetilde{B}\widetilde{\Phi}$. But $\widetilde{A}$ and $\widetilde{B}$ are co-prime and $\widetilde{A} \nmid \widetilde{\Phi}$, so this amounts to $k \not\equiv 0 \pmod{p}$.

Filtration degree

To prove (3),

$$f = \Phi(Q, R) \implies f^i = \Phi^i(Q, R).$$

Because $\widetilde{A}$ has no repeated factors, $\widetilde{A} \nmid \widetilde{\Phi}$ implies $\widetilde{A} \nmid \widetilde{\Phi}^i$.

Proof of main theorem

Goal

$$f \equiv f' \pmod{p^m} \implies k \equiv k' \pmod{p^{m-1}(p-1)}.$$

- $k \equiv k' \pmod{p-1}$ simply follows from $f \equiv f' \pmod{p}$.
- If $m = 1$, there is nothing else to show, so suppose $m \geq 2$.
- Recall the Eisenstein series

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

and Clausen–von Staudt theorem

$$(p-1) \mid k \implies v_p\left(\frac{2k}{B_k}\right) = 1 + v_p(k).$$

Proof of main theorem

- $E_k \equiv 1 \pmod{p^n} \iff p^{n-1}(p-1) \mid k$.
- Replacing f' with $f' E_{p^{n-1}(p-1)}$ for n large enough (so that none of the congruences above is affected), we may assume $h := k' - k \geq 4$.
- Let $r := v_p(h) + 1$.

Goal

Show $r \geq m$.