p-adic modular forms

TCC (Spring 2021), Lecture 1

Pak-Hin Lee

21st January 2021

Email me

Email me about yourself:

- Name, institution, year
- Credit or audit?
- Backgrounds in modular forms and algebraic geometry
- (Optional) Research interests; what you want to get out of this course

Plan

1. p-adic modular forms à la Serre [$4 - \epsilon$ lectures]
   - mod p modular forms, following Swinnerton-Dyer
   - p-adic modular forms, following Serre
   - some applications
2. p-adic modular forms à la Katz [$4 + \epsilon$ lectures]
   - crash course on algebro-geometric backgrounds
   - selected parts of Katz's article (depending on time, interests, etc.)
   - some applications

References

Main references:

- Swinnerton-Dyer
- Serre
- Katz

These were published in the same proceedings (LNM 350), available via Springer Link.

Prerequisites

- Familiarity with modular forms
- Familiarity with p-adic numbers
- Exposure to algebraic geometry in the language of schemes, and willingness to pick things up on the go

Today will be nice and easy, but we will gradually pick up the pace!

Modular forms

- Denote by $M_{k,\mathbf{C}}$ the space of modular forms of weight k and level 1.
- Identify $M_{k,\mathbf{C}} \subset \mathbf{C}[[q]]$ via q-expansions.
- For any ring $\mathbf{Z} \subset R \subset \mathbf{C}$, set $M_{k,R} := M_{k,\mathbf{C}} \cap R[[q]]$, the modular forms with Fourier coefficients in R.

Theorem (Integral structure)

$M_{k,R}$ contains a $\mathbf{C}$-basis of $M_{k,\mathbf{C}}$, i.e.

$$M_{k,\mathbf{C}} = M_{k,R} \otimes_R \mathbf{C}.$$

Eisenstein series

Recall the weight k Eisenstein series

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

where $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$.

Eisenstein series

Facts:

- For $k \geq 4$ even, G_k and E_k are modular forms of weight k.
- The algebra of modular forms of level 1 is generated by E_4 and E_6:
$$\bigoplus_{k \geq 4} M_{k,\mathbf{C}} = \mathbf{C}[E_4, E_6].$$

Remark

E_2 is *not* a modular form, but will play an important role.

Eisenstein series

Relations among modular forms amounts to comparing their constant terms:

Example

- $\dim M_{8,\mathbf{C}} = 1 \implies E_8 = E_4^2$.
- $\dim M_{10,\mathbf{C}} = 1 \implies E_{10} = E_4 \cdot E_6$.
- The unique normalized cusp form of weight 12 is $\Delta = \dfrac{1}{1728}(E_4^3 - E_6^2)$.

Modular forms mod p

- From now on, let $p \geq 5$ be a fixed prime (so that dividing by $1728 = 2^6 3^3$ is okay).
- Let $\mathbf{Z}_{(p)} = \{\frac{a}{b} \in \mathbf{Q} : (a, b) = 1, p \nmid b\}$ be the localization of $\mathbf{Z}$ at (p) (so that reduction mod p is okay).
- For $f \in M_{k,\mathbf{Z}_{(p)}}$ (p-integral Fourier coefficients), denote by $\widetilde{f}$ its image under reduction mod p:

$$\begin{aligned} M_{k,\mathbf{Z}_{(p)}} &\to \mathbf{F}_p[[q]] \\ f &\mapsto \widetilde{f}. \end{aligned}$$

Modular forms mod p

Define the space of "mod p modular forms" of weight k

$$\widetilde{M}_k := \{\widetilde{f} : f \in M_{k,\mathbf{Z}_{(p)}}\} \subset \mathbf{F}_p[[q]]$$

and the algebra of "mod p modular forms"

$$\widetilde{M} := \sum_k \widetilde{M}_k \subset \mathbf{F}_p[[q]].$$

Remark

This is *a priori* not a direct sum, because modular forms of different weights may be equal under reduction mod p (as we shall see in a moment).

Eisenstein series

For $k \geq 4$ even, recall the normalized Eisenstein series

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

where $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$.

Eisenstein series of weight $p-1$

Fact about Bernoulli numbers:

Theorem (Clausen–von Staudt)

If $(p-1) \mid k$, then $v_p(B_k) = -1$.

In particular, this implies

$$E_{p-1} = 1 - \frac{2(p-1)}{B_{p-1}} \sum_{n=1}^{\infty} \sigma_{p-2}(n) q^n$$

is congruent to 1 mod p, i.e. $\widetilde{E}_{p-1} = 1 \in \mathbf{F}_p[[q]]$.

$\widetilde{E}_{p-1} = 1$

This gives a non-trivial congruence between modular forms of weights $k-1$ and 0, so $\widetilde{M} = \sum_k \widetilde{M}_k$ is *not* a direct sum, and there is no natural $\mathbf{Z}$-grading on this subalgebra of $\mathbf{F}_p[[q]]$.
More precisely, we get a chain of inclusions

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

Are there other (more complicated) relations?

Goal

Systematically study the structure of mod p modular forms.

Ramanujan's convention

$$
\begin{aligned}
P &:= E_2 = 1 - 24 \sum \sigma_1(n) q^n, \\
Q &:= E_4 = 1 + 240 \sum \sigma_3(n) q^n, \\
R &:= E_6 = 1 - 504 \sum \sigma_5(n) q^n,
\end{aligned}
$$

so that

$$
\begin{aligned}
\Delta &= \frac{1}{1728}(Q^3 - R^2) \\
&= q - 24q^2 + \cdots .
\end{aligned}
$$

Modular forms

Lemma

$$\bigoplus_{k\geq 4} M_{k,\mathbf{Z}_{(p)}} = \mathbf{Z}_{(p)}[Q,R].$$

In particular, every $f \in M_{k,\mathbf{Z}_{(p)}}$ can be written as $f = F(Q,R)$ for some unique polynomial $F \in \mathbf{Z}_{(p)}[X,Y]$.

Proof.

This follows by induction: If $f \in M_{k,\mathbf{Z}_{(p)}}$ has constant term a, then $f - aQ^iR^j$ is a cusp form (for suitable i,j) and we have

$$\frac{f - aQ^iR^j}{\Delta} \in \mathbf{Z}_{(p)}[[q]] \cap M_{k-12,\mathbf{Z}_{(p)}}.$$

□

The polynomial A

Definition

Define $A \in \mathbf{Z}_{(p)}[X, Y]$ to be the polynomial such that $E_{p-1} = A(Q, R)$, and $\widetilde{A} \in \mathbf{F}_p[X, Y]$ to be its reduction mod p.

If we assign X and Y weights 4 and 6 respectively, then A is homogeneous of weight $p - 1$. Note that $A \neq 0$!

Remark

We will see that $\widetilde{A}$ is the Hasse invariant.

Structure of mod p modular forms

- Recall the algebra of mod p modular forms $\widetilde{M} = \sum_k \widetilde{M}_k \subset \mathbf{F}_p[[q]]$.
- There is a surjection $\mathbf{F}_p[X, Y] \to \widetilde{M}$ sending $X \mapsto \widetilde{Q}$, $Y \mapsto \widetilde{R}$.
- The relation $\widetilde{E}_{p-1} = 1$ means $\widetilde{A} - 1$ lies in the kernel.
- Swinnerton-Dyer: This is essentially the only congruence among modular forms (of level 1)!

Structure of mod p modular forms

Theorem (Swinnerton-Dyer)

The map $\mathbf{F}_p[X, Y] \to \widetilde{M}$ sending $X \mapsto \widetilde{Q}$, $Y \mapsto \widetilde{R}$ induces an isomorphism

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

of $\mathbf{F}_p$-algebras.

Remark

There is a different description for $p = 2, 3$.

An example

Example ($p = 11$)

- $E_{10} = QR$, so the polynomial A is just XY.
- Hence $\widetilde{M} = \mathbf{F}_{11}[X, Y]/(XY - 1)$.
- Geometrically, $\widetilde{M}$ is a Dedekind domain and $\operatorname{Spec} \widetilde{M} = \mathbf{P}^1 - \{0, \infty\}$ is a smooth affine curve over $\mathbf{F}_{11}$.

Structure of mod p modular forms

Let $\mathfrak{a}$ be the kernel of $\mathbf{F}_p[X, Y] \to \widetilde{M}$, i.e. there is an exact sequence

$$0 \longrightarrow \mathfrak{a} \longrightarrow \mathbf{F}_p[X, Y] \xrightarrow[\substack{X \mapsto \widetilde{Q} \\ Y \mapsto \widetilde{R}}]{} \widetilde{M} \longrightarrow 0$$

Goal

Show that $\mathfrak{a}$ is the principal ideal $(\widetilde{A} - 1)$.

Structure of mod p modular forms

Some (basic) commutative algebra:

- $\mathbf{F}_p[X, Y]$ has Krull dimension 2, with a chain of ideals

$$0 \subsetneq (\widetilde{A} - 1) \subset \mathfrak{a} \subsetneq \mathbf{F}_p[X, Y].$$

- $\mathfrak{a}$ is a prime ideal, since $\widetilde{M} \subset \mathbf{F}_p[[q]]$ is an integral domain.
- $\mathfrak{a}$ is not a maximal ideal; otherwise, the quotient $\widetilde{M}$ would be a field and $\widetilde{Q}, \widetilde{R} \in \mathbf{F}_p[[q]]$ would be algebraic, but at least one of them is not a constant power series (recall $Q = 1 + 240q + \cdots$, $R = 1 - 504q + \cdots$, and $p \geq 5$!).
- It suffices to show that $(\widetilde{A} - 1)$ is prime.

Proof: Irreducibility of $\widetilde{A} - 1$

In fact, we will show that $\widetilde{A} - 1$ is absolutely irreducible:

Lemma

$\widetilde{A} - 1$ is irreducible in $\overline{\mathbf{F}_p}[X, Y]$.

- Suppose $\Phi(X, Y)$ is a non-trivial irreducible factor of $\widetilde{A} - 1$.
- We may assume the constant term of Φ is 1 and write

$$\Phi(X, Y) = 1 + \Phi_1(X, Y) + \cdots + \Phi_n(X, Y)$$

where Φ_i is homogeneous of weight i (recall X, Y have weights $4, 6$ respectively).

Proof: Irreducibility of $\widetilde{A}-1$

- Choose a generator c of $\mathbf{F}_p^\times = \langle c \rangle$. Since $\widetilde{A}$ is homogeneous of weight $p-1$, we have

$$\widetilde{A}(c^4X, c^6Y) = \widetilde{A}(X, Y).$$

Remark

Swinnerton-Dyer considers $\widetilde{A}(c^2X, c^3Y)$, which is not quite correct as it gives $-\widetilde{A}(X, Y)$.

- Then $\Phi(c^4X, c^6Y)$ is also a factor of $\widetilde{A}-1$ distinct from $\Phi(X, Y)$, so

$$\Phi(c^4X, c^6Y)\Phi(X, Y) \mid \widetilde{A}-1.$$

Proof: Irreducibility of $\widetilde{A} - 1$

- By homogeneity, the highest weight term is

$$\Phi_n(c^4 X, c^6 Y)\Phi_n(X, Y) = c^n \Phi_n(X, Y)^2.$$

- Comparing the highest weight terms gives $\Phi_n(X, Y)^2 \mid \widetilde{A}$.

This would give a contradiction if we can show:

Lemma

$\widetilde{A} \in \mathbf{F}_p[X, Y]$ has no repeated factors.

To prove this, we need to introduce some differential operators on the space of modular forms.