# $p$-adic modular forms

## TCC (Spring 2021), Lecture 5

Pak-Hin Lee

18th February 2021

# Administrative issues

Slides:

- Lectures 1-4: available on webpage
- Lecture 4 includes a corrected discussion of the special values $\zeta^*(1-k)$ on P.21-24.

Problem sheets:

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

# Administrative issues

Office hours:

- Time: starting next week
- Format: Q&A? Tutorial? Supplementary lectures?
- Content: Problem sheets? Geometric modular forms?

Email:

- Personal replies: I still owe many of you!
- Survey: office hours, feedback, etc.

# Plans

Today (mostly):

- Recap
- Hecke operators on $p$-adic modular forms
- Applications of $U_p$-operator: constant terms; congruences
- Note: I want to illustrate two important principles, while omitting many details.

Today (briefly):

- Weierstrass parametrization of elliptic curves over $\mathbf{C}$
- Crash course on geometric modular forms: next week (possibly during office hours?)

# Recap: $p$-adic modular forms

- $f \in \mathbf{Q}_p[[q]]$ is a **(Serre)** $p$**-adic modular form** if it is the limit of a sequence of classical modular forms $f_i \in M_{k_i,\mathbf{Q}}$.
- $f$ has a well-defined notion of **weight**: $k_i$ converges to $k \in \mathfrak{X} = \mathbf{Z}_p \times \mathbf{Z}/(p-1)\mathbf{Z}$ (group of characters of $\mathbf{Z}_p^\times$).
- **Slogan:** The non-constant coefficients $a_n$ (for $n \geq 1$) govern the constant term $a_0$.

## Example

- $p$-adic Eisenstein series $G_k^*$
- $p$-adic zeta function $\zeta^*(s)$
- Today: formula for $a_0$ in certain cases

# Hecke operators $T_\ell$ for $\ell \neq p$

- Recall **Hecke operators** on classical modular forms: If $f = \sum_{n=0}^{\infty} a_n q^n \in M_k$, then for $\ell$ prime,

$$f|_k T_\ell = \sum_{n=0}^{\infty} a_{n\ell} q^n + \ell^{k-1} \sum_{n=0}^{\infty} a_n q^{n\ell} \in M_k.$$

- Recall: for each fixed $d \in \mathbf{Z}_p^\times$, the map $\mathfrak{X} \to \mathbf{Q}_p^\times$, $k \mapsto d^k$ is continuous.
- Last week: $T_\ell$ behaves well under $p$-adic limits so long as $\ell \neq p$. (More precisely, if $f_i \in M_{k_i}$ tends to $f \in M_k^\dagger$, then $f_i|_{k_i} T_\ell \in M_{k_i}$ tends to $f|_k T_\ell \in M_k^\dagger$ given by the same formula.)
- Hence for $\ell \neq p$, $T_\ell$ acts on $f = \sum_{n=0}^{\infty} a_n q^n \in M_k^\dagger$ by

$$f|_k T_\ell := \sum_{n=0}^{\infty} a_{n\ell} q^n + \ell^{k-1} \sum_{n=0}^{\infty} a_n q^{n\ell} \in M_k^\dagger.$$

# Hecke operator $U_p$

For $\ell = p$, the behavior of $p^{k_i - 1}$ is erratic even when $k_i \to k \in \mathfrak{X}$.

## Idea

- We have seen that every sequence $k_i \in \mathbf{Z}$ tending to $k \in \mathfrak{X}$ can be replaced by one for which $k_i \to \infty$ in $\mathbf{R}$.
- This can be done even for a sequence $f_i \in M_{k_i}$ tending to $f \in M_k^\dagger$, as follows.
- Since $E_{p^m(p-1)} \equiv 1 \pmod{p^{m+1}}$, replacing $f_i$ by $f_i \cdot E_{p^{m_i}(p-1)}$ (where $m_i \gg 0$) has the effect of replacing $k_i$ by $k_i + p^{m_i}(p-1)$, and therefore:
  - $f_i \to f$ in $\mathbf{Q}_p[[q]]$.
  - $k_i \to k$ in $\mathfrak{X}$.
  - $k_i \to \infty$ in $\mathbf{R}$.

  This trick can always be applied to ensure $k_i \to \infty$, whenever we have $f_i \in M_{k_i}$ tending to $f \in M_k^\dagger$.

# Hecke operator $U_p$

The condition $k_i \to \infty$ implies $p^{k_i-1} \to 0 \in \mathbf{Q}_p$, so

$$f_i|_{k_i} T_p = \sum_{n=0}^{\infty} a_{np}^{(i)} q^n + p^{k_i-1} \sum_{n=0}^{\infty} a_n^{(i)} q^{np} \in M_{k_i}$$

tends to

$$f|U_p := \sum_{n=0}^{\infty} a_{np} q^n.$$

Hence this defines a $p$-adic modular form of weight $k = \lim k_i$.

**Remark (Notation)**

For classical modular forms of level $N$ divisible by $p$, $T_p$ is denoted by $U_p$ and $f|U_p$ is given by the same formula.

# Hecke operator $V_p$

## Question

What about the part $f|V_p := \sum_{n=0}^{\infty} a_n q^{np}$?

## Remark (Notation)

Classically, the level-raising operator $(f|V_p)(z) := f(pz)$ is given by the same formula.

As formal power series in $\mathbf{Q}_p[[q]]$, we have

$$f_i|V_p = p^{1-k_i}(f_i|_{k_i}T_p - f_i|U_p),$$

where:

- $f_i|_{k_i}T_p \in M_{k_i}$ is a **classical** modular form;
- $f_i|U_p \in M_{k_i}^{\dagger}$ is a $p$-**adic** modular form.

Thus $f_i|V_p \in M_{k_i}^{\dagger}$.

# Hecke operator $V_p$

Now

$$f_i|V_p = \sum_{n=0}^{\infty} a_n^{(i)} q^{np} \in M_{k_i}^{\dagger}$$

tends to

$$f|V_p = \sum_{n=0}^{\infty} a_n q^{np}.$$

Hence this defines a $p$-adic modular form of weight $k = \lim k_i$.

**Remark**

This is slightly tricky: $f|V_p$ is more readily seen as a limit of $p$-adic modular forms (rather than classical modular forms).

# Hecke operators on $p$-adic modular forms

## Definition (Hecke operators)

Let $f = \sum_{n=0}^{\infty} a_n q^n \in \mathbf{Q}_p[[q]]$. Define

$$f|U_p := \sum_{n=0}^{\infty} a_{np} q^n,$$

$$f|V_p := \sum_{n=0}^{\infty} a_n q^{np}.$$

If $\ell \neq p$ is a prime and $k \in \mathfrak{X}$, define

$$f|_k T_\ell := \sum_{n=0}^{\infty} a_{n\ell} q^n + \ell^{k-1} \sum_{n=0}^{\infty} a_n q^{n\ell}.$$

# Hecke operators on $p$-adic modular forms

We have shown:

**Theorem (théorème 4, P.209)**

*If $f$ is a $p$-adic modular form of weight $k \in \mathfrak{X}$, then so are $f|U_p$, $f|V_p$ and $f|_k T_\ell$ for any prime $\ell \neq p$.*

# Example: $p$-adic Eisenstein series

Recall the $p$-adic Eisenstein series

$$G_k^* = \frac{1}{2}\zeta^*(1-k) + \sum_{n=1}^{\infty} \sigma_{k-1}^*(n) q^n \in M_k^\dagger.$$

Problem Sheet 2:

1. $G_k^* | T_\ell = (1 + \ell^{k-1}) G_k^*$.
2. $G_k^* | U_p = G_k^*$.
3. $G_k^* = G_k | (1 - p^{k-1} V_p)$ for $k \in \mathbf{Z}_{\geq 2}$ even.

(3) can be used to show:

- $\zeta^*(1-k) = (1 - p^{k-1})\zeta(1-k)$ for $k \in \mathbf{Z}_{\geq 2}$ even.
- $E_2$ is a $p$-adic modular form of weight 2.

# Theta operators on $p$-adic modular forms

Recall the theta operator:

- $\Theta$ almost acts on classical modular forms, up to a factor of $P$.
- $\Theta$ acts on mod $p$ modular forms $\widetilde{M}$.

**Theorem (théorème 5, P.211)**

*If $f = \sum a_n q^n$ is a p-adic modular form of weight $k \in \mathfrak{X}$, then:*

1. $$\Theta f := q\frac{df}{dq} = \sum_{n=0}^{\infty} n a_n q^n$$
   *is a p-adic modular form of weight $k+2$.*
2. *For $h \in \mathfrak{X}$,*
   $$f|R_h := \sum_{(n,p)=1} n^h a_n q^n$$
   *is a p-adic modular form of weight $k+2h$.*

# Motivation

**Idea**

**Slogan:** The $U_p$-operator has a good spectral theory.

- For Serre $p$-adic modular forms, this follows from a **contraction property** of $U_p$ on mod $p$ modular forms, which controls the filtration degree $w(\widetilde{f})$.
- In the geometric theory, we will see that $U_p$ is a **compact** (or "completely continuous") operator.

# $U_p$-operator on mod $p$ modular forms

On classical modular forms of weight $k$ (and level 1),

$$f|_k T_p = \sum_{n=0}^{\infty} a_{np} q^n + p^{k-1} \sum_{n=0}^{\infty} a_n q^{np} \in M_k.$$

Reduction mod $p$ gives

$$f|_k T_p \equiv \sum_{n=0}^{\infty} a_{np} q^n = f|U_p \pmod{p}.$$

This shows $U_p$ defines an operator on $\widetilde{M}_k$, and hence on

$$\widetilde{M}^{\alpha} = \bigcup_{k \equiv \alpha \pmod{p-1}} \widetilde{M}_k, \quad \alpha \in \mathbf{Z}/(p-1)\mathbf{Z}.$$

# Contraction property of $U_p$

The $U_p$-operator satisfies the following contraction property.

## Theorem (théorème 6, P.212)

1. *If* $k > p+1$, *then* $U_p(\widetilde{M}_k) \subset \widetilde{M}_{k'}$ *for some* $k' < k$.
2. $U_p : \widetilde{M}_{p-1} \to \widetilde{M}_{p-1}$ *is an isomorphism.*

## Remark

Note that in (1), we necessarily have $k' \equiv k \pmod{p-1}$ by the structure theorem

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

# Contraction property of $U_p$

Picture:

- Recall the filtration on $\widetilde{M}^\alpha$

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

- Start with any $\widetilde{f} \in \widetilde{M}_k$.
- Applying $U_p$ brings it down the filtration.
- Repeating this, $U_p^m \widetilde{f}$ lands in $\widetilde{M}_{k'}$ for some $k' \leq p+1$.
- The space $\widetilde{M}_{k'}$ is finite-dimensional!

# Proof of contraction property

The proof uses the filtration degree $w(\widetilde{f})$. As usual, let $p \geq 5$.

**Lemma (lemme 2, P.213)**

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

1. $w(\widetilde{f}|U_p) \leq p + \dfrac{w(\widetilde{f}) - 1}{p}$.
2. *If $w(\widetilde{f}) = p - 1$, then $w(\widetilde{f}|U_p) = p - 1$.*

See Serre for the proofs of:

- lemme 2;
- lemme 2 $\implies$ théorème 6.

# Some linear algebra

## Lemma

*Let $V$ be a finite-dimensional vector space and $T$ be an operator on $V$. Then there is a unique decomposition*

$$V = S \oplus N$$

*such that $T$ is bijective on $S$ and nilpotent on $N$.*

## Proof.

Let $d = \dim V$. Then define

$$S := \bigcap_{i=1}^{\infty} \mathrm{im}(T^i) = \mathrm{im}(T^d),$$

$$N := \bigcup_{i=1}^{\infty} \ker(T^i) = \ker(T^d).$$

# Spectral decomposition of mod $p$ modular forms

In general this cannot be done for infinite-dimensional spaces, but the contraction property of $U_p$ allows for an analogous decomposition of $\widetilde{M}^\alpha$.

**Theorem (corollaire, P.214)**

*Let $p \geq 5$ and $\alpha \in \mathbf{Z}/(p-1)\mathbf{Z}$ be even.*

- *There is a unique decomposition*

$$\widetilde{M}^\alpha = \widetilde{S}^\alpha \oplus \widetilde{N}^\alpha$$

  *such that $U_p$ is bijective on $\widetilde{S}^\alpha$ and locally nilpotent on $\widetilde{N}^\alpha$.*
- *$\widetilde{S}^\alpha \subset \widetilde{M}_j$, where $j \in \alpha$ is such that $4 \leq j \leq p+1$. In particular, $\widetilde{S}^\alpha$ is finite-dimensional.*
- *For $\alpha = 0$, we have $\widetilde{S}^0 = \widetilde{M}_{p-1}$.*

# Spectral decomposition of mod $p$ modular forms

## Remark

- $\widetilde{S}^\alpha$ is called the **ordinary part** of $\widetilde{M}^\alpha$, and is the image of the **ordinary projector** $e = \lim_{n\to\infty} U_p^{n!}$ on $\widetilde{M}^\alpha$.
- "**Locally nilpotent** on $\widetilde{N}^\alpha$" means for every $v \in \widetilde{N}^\alpha$, there exists $m \in \mathbf{Z}$ such that $U_p^m v = 0$ (note that $m$ depends on $v$ because $\widetilde{N}^\alpha$ is infinite-dimensional).
- There is a similar statement for $p = 2$ or $3$, which we omit.

# Spectral decomposition of mod $p$ modular forms

This has the following implication for $p$-adic modular forms.

- For mod $p$ modular forms, $U_p$ is **locally nilpotent** on $\widetilde{N}^{\alpha}$.
- For $p$-adic modular forms, $U_p$ is **topologically nilpotent** on the preimage of $\widetilde{N}^{\alpha}$.

**Lemma (generalizing lemme 3, P.216)**

*If $g \in M_k^{\dagger}$ with $\widetilde{g} \in \widetilde{N}^{\alpha}$, then*

$$\lim_{m \to \infty} g | U_p^m = 0.$$

See Problem Sheet 2.

# Application: Constant terms

**Recurring theme:** The non-constant coefficients of a $p$-adic modular form control its constant term.

**Theorem (théorème 7, P.215; remarque, P.216)**

*Let* $f = \sum_{n=0}^{\infty} a_n(f)q^n \in M_k^\dagger$ *with* $k \neq 0 \in \mathfrak{X}$ *and* $k \equiv 4, 6, 8, 10, 14 \pmod{p-1}$*. Then*

$$a_0(f) = \frac{1}{2}\zeta^*(1-k) \lim_{n\to\infty} a_{p^n}(f).$$

- $p \leq 7$: stated and proved in théorème 7; condition on $k \pmod{p-1}$ is automatic
- $p \geq 11$: stated in remarque; follows a similar argument

# Application: Constant terms

Proof sketch:

- The condition on $k \pmod{p-1}$ guarantees that the ordinary part $\widetilde{S}^\alpha$ is one-dimensional and spanned by $\widetilde{E}_{k_0}$ where $k_0 \in \{4, 6, 8, 10, 14\}$.
- Write
$$f = \frac{a_0(f)}{\frac{1}{2}\zeta^*(1-k)} G_k^* + g$$
where $g$ is a cusp form (i.e. $a_0(g) = 0$).
- Under the decomposition $\widetilde{M}^\alpha = \widetilde{S}^\alpha \oplus \widetilde{N}^\alpha$, we see that
$$\widetilde{g} \in \widetilde{N}^\alpha.$$

# Application: Constant terms

Proof sketch (continued):

- Show the formula for $G_k^*$ and $g$ respectively.
- For $G_k^*$, this is clear from its explicit formula:

$$a_0(G_k^*) = \frac{1}{2}\zeta^*(1-k),$$
$$a_{p^n}(G_k^*) = \sigma_{k-1}^*(p^n) = 1.$$

- For $g$ with $\widetilde{g} \in \widetilde{N}^\alpha$, this follows from the topological nilpotence of $U_p$:

$$\lim_{m\to\infty} g|U_p^m = 0;$$

taking the Fourier coefficient at $n = 1$ gives

$$a_1(g|U_p^m) = a_{p^m}(g).$$

# Application: Constant terms

## Remark

- For general $f \in M_k^\dagger$ with $k \neq 0$, there exists a (complicated!) universal formula for calculating $a_0(f)$ in terms of $a_n(f)$ – see Serre's discussion on P.217-222.
- The complication is caused by the fact that the ordinary part $\widetilde{S}^\alpha$ is not necessarily one-dimensional.
- This would make a good project for those of you interested in the computational aspects of $p$-adic modular forms.

# Application: Congruences for $j$-invariant

Take as black box the main result of §3:

**Theorem (théorème 10, P.226; remarque, P.228)**

*Let $f = \sum a_n q^n$ be a (meromorphic) modular form of weight $k$ on $\Gamma_0(p)$ with $a_n \in \mathbf{Q}$, which is holomorphic at $\infty$ and meromorphic at 0. Then $f$ is a $p$-adic modular form of weight $k$.*

**Remark**

$\Gamma_0(p)$ has two cusps at $\infty$ and 0.

**Idea**

**Slogan:** $p$-adic modular forms of level $N$ see all classical forms of level $Np^m$.

# Application: Congruences for $j$-invariant

## Example

The $j$-invariant

$$j(z) = q^{-1} + 744 + \sum_{n=1}^{\infty} c(n) q^n, \quad c(n) \in \mathbf{Z}$$

is a meromorphic modular function on $\mathrm{SL}_2(\mathbf{Z})$, with a simple pole at $\infty$. Now

$$(j|U_p)(z) = 744 + \sum_{n=1}^{\infty} c(pn) q^n$$

is a meromorphic modular function on $\Gamma_0(p)$, with a pole of order $p$ at 0. Thus the theorem implies

$$j|U_p \in M_0^{\dagger}.$$

# Application: Congruences for $j$-invariant

Recall that Lehner (1949) and Atkin (1966) imply:

**Theorem**

*For $p \leq 11$ and $n \in \mathbf{Z}_{\geq 1}$, $c(p^m n) \to 0$ in $\mathbf{Q}_p$ as $m \to \infty$.*

**Proof.**

We have seen that $j|U_p \in M_0^\dagger$. For $\alpha = 0 \in \mathbf{Z}/(p-1)\mathbf{Z}$,

$$\widetilde{M}^0 = \widetilde{S}^0 \oplus \widetilde{N}^0 \overset{\text{by } \alpha=0}{=} \widetilde{M}_{p-1} \oplus \widetilde{N}^0 \overset{\text{by } p\leq 11}{=} \mathbf{F}_p \oplus \widetilde{N}^0,$$

so that $j|U_p - 744 \in \widetilde{N}^0$. By the previous lemma,

$$(j|U_p - 744)|U_p^m \to 0 \text{ as } m \to \infty,$$

i.e. $(j - 744)|U_p^m \to 0$. Its $n$-th Fourier coefficient is $c(p^m n)$. □

# Geometric modular forms

**Goal**

Interpret modular forms using algebraic geometry.

- Complex analysis: Modular forms are initially defined as holomorphic functions on $\mathbf{H}$ satisfying a transformation property.
- Lattices: Interpret as functions on lattices $\Lambda \subset \mathbf{C}$.
- Weierstrass parametrization: Interpret as functions on elliptic curves over $\mathbf{C}$ (with additional data).
- Algebraic geometry: Generalize this for elliptic curves over any ring (or scheme).

# Elliptic curves over $\mathbf{C}$

Weierstrass parametrization: For a lattice $\Lambda \subset \mathbf{C}$, the complex torus $\mathbf{C}/\Lambda$ has the structure of an elliptic curve with equation

$$y^2 = 4x^3 - 60G_4(\Lambda)x - 140G_6(\Lambda)$$

where

$$G_{2k}(\Lambda) := \sum_{\lambda \in \Lambda - \{0\}} \frac{1}{\lambda^{2k}}.$$

The isomorphism is given by

$$x = \wp(z;\Lambda) := \frac{1}{z^2} + \sum_{\lambda \in \Lambda - \{0\}} \left( \frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right),$$

$$y = \wp'(z;\Lambda) = -\sum_{\lambda \in \Lambda} \frac{2}{(z-\lambda)^3}.$$

# Elliptic curves over C

- Homothety: Two lattice $\Lambda$ and $\Lambda'$ are homothetic, denoted $\Lambda \sim \Lambda'$ if $\Lambda = \mu\Lambda'$ for some $\mu \in \mathbf{C}^\times$.
- Two homothetic lattices give rise to isomorphic elliptic curves, and vice versa:

$$\Lambda \sim \Lambda' \iff \mathbf{C}/\Lambda \cong \mathbf{C}/\Lambda'.$$

- Weierstrass parametrization: There is a bijection

$$\{\text{Lattices in } \mathbf{C}\}/\sim \;\longleftrightarrow\; \{\text{Elliptic curves over } \mathbf{C}\}/\cong$$
$$\Lambda \longmapsto \mathbf{C}/\Lambda.$$

# Modular forms as functions on lattices

- Every lattice is homothetic to one of the form

$$\mathbf{Z}\tau + \mathbf{Z}, \quad \tau \in \mathbf{H}.$$

- We have

$$\mathbf{Z}\tau + \mathbf{Z} \sim \mathbf{Z}\tau' + \mathbf{Z} \iff \tau' = \frac{a\tau + b}{c\tau + d}, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}).$$

- Modular forms of weight $k$ can be interpreted as functions on lattices satisfying

$$F(\mu\Lambda) = \mu^{-k} F(\Lambda).$$

  This correspondence is given by $f(\tau) = F(\mathbf{Z}\tau + \mathbf{Z})$.

**Example**

$$G_{2k}(\mu\Lambda) = \mu^{-2k} G_{2k}(\Lambda).$$