Classicality Theorems of p-adic modular forms

Chi-Yun Hsu

University of California, Los Angeles

Santa Clara University
January 26, 2022

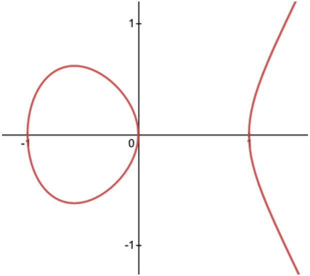
Elliptic curves

An elliptic curve E is defined by a degree 3 equation

$$E\colon y^2 = x^3 + ax + b,$$

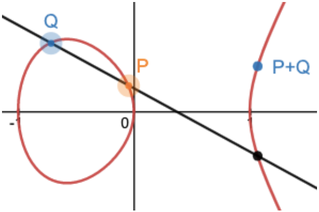
where $x^3 + ax + b$ has no repeated roots.
For example,

$$E\colon y^2 = x^3 - x$$



Additive group law on elliptic curves

It makes sense to add two points on an elliptic curve.



For example,

$$(0,0) + (1,0) = (-1,0)$$
$$(0,0) + (0,0) = \infty,$$

so we always include the infinity point ∞ with an elliptic curve.
The addition on elliptic curves is used in cryptography.

Elliptic curve modulo p

Can consider points modulo a prime number p.

$$E\colon y^2 = x^3 - x$$

- When $p = 2$, the x-coordinate has two possibilities $x = 0, 1$.
  When $x = 0$, we have $y = 0$.
  When $x = 1$, we have $y = 0$.
  So there are 3 points modulo $p = 2$:
  $$E(\mathbb{F}_2) = \{\infty, (0,0), (1,0)\}$$
- When $p = 3$, the x-coordinate has three possibilities $x = 0, 1, 2$.
  When $x = 0$, we have $y = 0$.
  When $x = 1$, we have $y = 0$.
  When $x = 2$, we have $y = 0$.
  So there are 4 points modulo $p = 3$:
  $$E(\mathbb{F}_3) = \{\infty, (0,0), (\pm 1, 0)\}$$

Elliptic curves and modular forms

We can associate a power series

$$f(q) = q + a_2 q^2 + a_3 q^3 + \cdots$$

where $a_p = (p+1) - \#E(\mathbb{F}_p)$, $a_{p^r} = a_{p^{r-1}} a_p - \underline{p a_{p^{r-2}}}$, and $a_{mn} = a_m a_n$ if $gcd(m,n) = 1$.

- $p = 2$: $E(\mathbb{F}_2) = \{\infty, (0,0), (1,0)\}$
  $a_2 = (2+1) - 3 = 0$
- $p = 3$: $E(\mathbb{F}_3) = \{\infty, (0,0), (\pm 1, 0)\}$
  $a_3 = (3+1) - 4 = 0$
- $p = 5$: $E(\mathbb{F}_5) = \{\infty, (0,0), (\pm 1, 0), (2, \pm 1), (-2, \pm 2)\}$
  $a_5 = (5+1) - 8 = -2$

The power series

$$f(q) = q - 2q^5 - 3q^9 + 6q^{13} + \cdots$$

turns out to be a modular form of weight 2.

Modularity Theorem

A modular form is some special power series

$$f(q) = a_0 + a_1 q + \cdots .$$

There is an invariant, called the weight $k \in \mathbb{Z}$, associated to f.

Modularity Theorem (Wiles 1994)

All semistable elliptic curves give a power series which is a modular form, i.e. all semistable elliptic curves are modular.

$$\Downarrow$$

Fermat's Last Theorem (stated 1637)

For $n \geq 3$, the equation

$$a^n + b^n = c^n$$

has no positive integer solution (a, b, c).

p-adic numbers

We can write integers in binary expansions:

$$\begin{array}{ccccccccc} 6 & = & & & 2 & + & 2^2 & & \\ 7 & = & 1 & + & 2 & + & 2^2 & & \\ 8 & = & & & & & & & 2^3 \end{array}$$

A 2-adic (p-adic) integer is an infinite series

$$a_0 + a_1 \cdot 2 + a_2 \cdot 2^2 + \cdots + a_n \cdot 2^n + \cdots$$
$$(a_0 + a_1 \cdot p + a_2 \cdot p^2 + \cdots + a_n \cdot p^n + \cdots)$$

where $a_n = 0$ or 1 ($a_n = 0, \ldots, p-1$).
For example, $1 + 2 + 2^2 + \cdots$ is a 2-adic integer but not an integer.

Alternatively, the ring of p-adic integers is $\mathbb{Z}_p := \varprojlim_r \mathbb{Z}/p^r\mathbb{Z}$,
i.e. congruence modulo p-powers and let the power go to infinity.

p-adic modular forms

To define p-adic modular forms, we take congruences of modular forms modulo p-powers and let the power go to infinity.

p-adic modular forms by example

Let $k \geq 4$ be an integer. Consider the Eisenstein series of weight k

$$G_k(q) := \frac{\zeta(1-k)}{2} + \sum_{n\geq 1} \sigma_{k-1}(n) q^n$$

where $\sigma_{k-1}(n) := \sum_{d|n} d^{k-1}$ and $\zeta(s) = \sum_{n\geq 1} n^{-s} = \prod_{\ell \text{ prime}} (1-\ell^{-s})^{-1}$.
Let $p \geq 3$ be a prime and consider

$$\begin{aligned} G_k^{(p)}(q) &:= G_k(q) - p^{k-1} G_k(q^p) \\ &= \frac{\zeta^{(p)}(1-k)}{2} + \sum_{n\geq 1} \sigma_{k-1}^{(p)}(n) q^n \end{aligned}$$

where $\sigma_{k-1}^{(p)}(n) := \sum_{d|n, p\nmid d} d^{k-1}$ and $\zeta^{(p)}(s) = \prod_{\ell \text{ prime}, \ell \neq p} (1-\ell^{-s})^{-1}$.
Then for each $r \geq 1$,

$$\begin{aligned} k \equiv k' \mod (p-1)p^{r-1} &\Longrightarrow d^{k-1} \equiv d^{k'-1} \mod p^r, \forall p \nmid d \\ &\Longrightarrow G_k^{(p)} \equiv G_{k'}^{(p)} \mod p^r \end{aligned}$$

p-adic modular forms by example

For each $r \geq 1$,

$$k \equiv k' \mod (p-1)p^{r-1} \Longrightarrow G_k^{(p)} \equiv G_{k'}^{(p)} \mod p^r$$

Given $\kappa = (k_r) \in \varprojlim_r \mathbb{Z}/(p-1)p^{r-1}\mathbb{Z}$, the topological limit

$$G_\kappa^{(p)} = \lim_{r\to\infty} G_{k_r}^{(p)} \in \mathbb{Z}_p[\![q]\!]$$

is a p-adic modular form of weight κ.

Classicality Theorem

Let $f = \sum_{n \geq 1} a_n q^n$ be a p-adic modular form of weight κ.

Question

When is f a classical modular form?

Necessary condition: When f is classical,

- the weight κ is an integer k
- $\mathrm{val}_p(a_p) \leq k - 1$, i.e., $p^\alpha \nmid a_p$ if $\alpha > k - 1$

Theorem (Coleman 1996)

Let $f = \sum_{n \geq 1} a_n q^n$ be an overconvergent p-adic modular form of weight $k \in \mathbb{Z}$. If

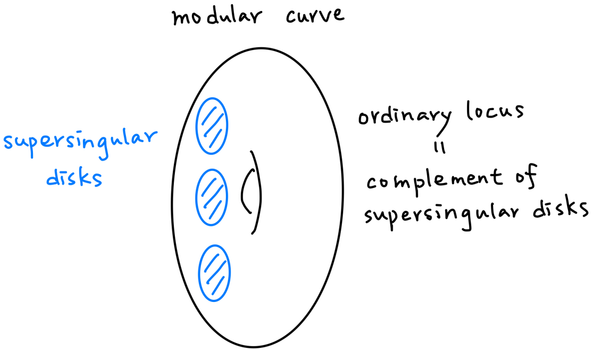
$$\mathrm{val}_p(a_p) < k - 1 \quad \textit{(small slope condition)},$$

then f is a classical modular form.

Overconvergent p-adic modular forms

Geometric perspective of modular forms

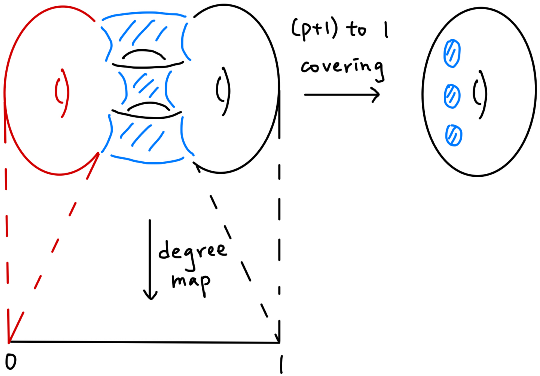
- Modular forms are "functions" on a modular curve
- Overconvergent p-adic modular forms are "functions" on a neighborhood of the ordinary locus of a modular curve



Overconvergent p-adic modular forms form a Fréchet space.

Buzzard's alternative idea for proving classicality

Goal: Extend the domain of definition to the whole modular curve



- The coefficient a_p is the eigenvalue of a compact Hecke operator U_p
- U_p strictly increases degree, except at degree 0 and 1.
- The extension to degree 0 is defined as an infinite series, which converges under the small slope condition.

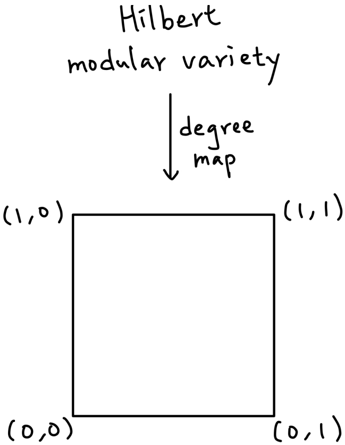
My work: Refined classicality for Hilbert modular forms

Let F be a totally real field, $[F : \mathbb{Q}] = n$.

Modular forms	$\rightsquigarrow$	Hilbert modular forms
weight k	$\rightsquigarrow$	weight $(k_1, \ldots, k_n)$
Modular curves	$\rightsquigarrow$	n-dim. Hilbert modular variety
Unit interval $[0, 1]$	$\rightsquigarrow$	Unit hypercube $[0, 1]^n$
U_p operator	$\rightsquigarrow$	$U_{\mathfrak{p}_1}, \ldots, U_{\mathfrak{p}_r}$ operators
		($r \leq n$ is determined by F and p)

My work: Refined classicality for Hilbert modular forms

For each $I \subseteq \{1, 2, \ldots, n\}$, can consider I-classical Hilbert modular forms. For example, when $n = 2$



$\varnothing$-classical = overconvergent, $\{1, 2, \ldots, n\}$-classical = classical

My work: Refined classicality for Hilbert modular forms

Theorem (H. 2021)

(Stated for $n = 2$ for simplicity) Assume that p is unramified. Let f be an overconvergent p-adic Hilbert modular form.

- *If* $\begin{cases} \mathrm{val}_p(a_p) < \min(k_1, k_2) - 2 & \text{when } r = 1 \\ \mathrm{val}_p(a_{\mathfrak{p}_i}) < k_i - 1, i = 1, 2 & \text{when } r = 2 \end{cases}$*, then f is classical.*
- *If* $\begin{cases} \mathrm{val}_p(a_p) < k_i - 2 & \text{when } r = 1 \\ \mathrm{val}_p(a_{\mathfrak{p}_i}) < k_i - 1 & \text{when } r = 2 \end{cases}$*, then f is i-classical.*

Future directions:

- Remove the assumption "p is unramified"
- Prove by Coleman's original cohomological method to obtain optimal slope bound.