Modular Forms

Hongyue Li

Modular Forms

A modular function of weight $2k$ is a meromorphic function on the upper half-plane and at infinity, $f : \mathbb{H} \cup \infty \to \mathbb{C}$, such that:

For all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ (i.e., 2×2 integer matrices with det 1),

$$f(\gamma z) = f\left(\frac{az+b}{cz+d}\right) = (cz+d)^{2k} f(z)$$

It is a modular form if it is holomorphic on $\mathbb{H}$ and at ∞.
Since $-I$ acts trivially, let the modular group be $PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm I\}$.

- Fourier expansion: $f(z) = \sum_{n=0}^{\infty} a_n q^n$, where $q = e^{2\pi i z}$
- Cusp forms: modular forms with $f(\infty) = 0$, equivalently $a_0 = 0$
- Denote M_k the complex vector space of modular forms of weight 2k, it has dimension dim $= \left\lfloor \frac{k}{6} \right\rfloor$ or $\left\lfloor \frac{k}{6} \right\rfloor + 1$

Let

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Then S and T generate $\mathrm{PSL}_2(\mathbb{Z})$.

The fundamental domain $\mathcal{D}$ of the modular group is:

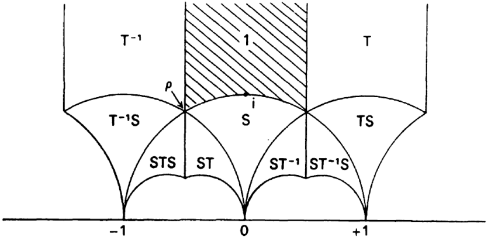


Figure 1: Fundamental Domain D of $\mathcal{H}$ under action of $\mathrm{SL}_2(\mathbb{Z})$.

$\mathcal{D} \to \mathbb{H}/\mathrm{PSL}_2(\mathbb{Z})$ is surjective and almost injective

Application: Little Picard Theorem

There is no non-constant holomorphic map $f : \mathbb{C} \to \mathbb{C} \setminus \{0, 1\}$

Proof:

$$U := \left\{ z \in \mathbb{C} \mid \Im z > 0,\ |z - \tfrac{1}{2}| > \tfrac{1}{2},\ 0 < \Re z < 1 \right\}$$

By the Riemann mapping theorem, there exists a conformal equivalence $f : U \to \mathbb{H}$ which extends continuously to ∂U and fixes 0 and 1.
By the Schwarz reflection principle and properties of the modular group, this extends to a covering map:

$$f : \mathbb{H} \to \mathbb{C} \setminus \{0, 1\}$$

Since $\mathbb{C}$ is simply connected, any holomorphic map $h : \mathbb{C} \to \mathbb{C} \setminus \{0, 1\}$ lifts to a map $\tilde{h} : \mathbb{C} \to \mathbb{H}$ such that the following diagram commutes:

$$\begin{array}{ccccc} & & \mathbb{H} & & \to \mathbb{D} \\ & \nearrow^{\tilde{h}} & \downarrow^{f} & & \\ \mathbb{C} & \xrightarrow{h} & \mathbb{C} \setminus \{0, 1\} & & \end{array}$$

By Liouville's theorem, $\tilde{h}$ is constant $\Rightarrow$ h is constant.

Elliptic Curves

Eisenstein series:
For a lattice $\Lambda_\tau = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \mathbb{Z} + \mathbb{Z}\tau$ with $\tau = \omega_2/\omega_1 \in \mathbb{H}$, the Einstein series of index k is a modular form of weight 2k:

$$G_k(\Lambda) = \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^{2k}} = \sum_{(m,n) \neq (0,0)} \frac{1}{(m\omega_1 + n\omega_2)^{2k}}$$

correspondence between lattice and elliptic curve over $\mathbb{C}$:

- Weierstrass $\wp$-function: $\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$
- elliptic curve: $E_\Lambda : y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$, where $x = \wp, y = \wp', g_2 = 60G_2, g_3 = 140G_3$
- modular discriminant: $\Delta(\tau) = g_2(\tau)^3 - 27g_3(\tau)^2$ is a cusp form of weight 12

Two elliptic curves $E_\tau \simeq E_{\tau'}$ iff $\exists \gamma \in PSL_2(\mathbb{Z})$ such that $\gamma\tau = \tau'$.
Moduli space of complex elliptic curves is $PSL_2(\mathbb{Z}) \backslash \mathbb{H}$.

The j-invariant

Definition: The j-invariant is a modular function of weight 0, defined as:

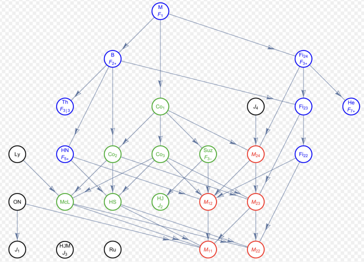
$$j(\tau) = 1728 \, \frac{g_2(\tau)^3}{\Delta(\tau)}$$

q-expansion:

$$j(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \cdots$$

properties:

- j is holomorphic on $\mathbb{H}$ with a simple pole at ∞.
- $j : \mathbb{H}/PSL_2(\mathbb{Z}) \to \mathbb{C}$ is a bijective holomorphic map.
- any modular function of weight 0 is a rational function of j
- two elliptic curves are isomorphic iff their j-invariants are equal



The Monster group $\mathbb{M}$ is the largest sporadic finite simple group:

- Order: $\approx 8 \times 10^{53}$
- The least number of dimensions in which the Monster group can act non-trivially is 196,883

Monstrous Moonshine: The coefficients of $j(\tau)$ are related to dimensions of irreducible representations of $\mathbb{M}$:

$$j(\tau) = q^{-1} + 744 + 196884q + \cdots, \quad 196884 = 196883 + 1$$

Theta Function

Let Λ be a lattice in an n-dimensional real vector space with inner product $(\cdot,\cdot)$. The associated theta function is defined by:

$$\theta_\Lambda(z) = \sum_{x\in\Lambda} e^{\pi i z(x,x)} = \sum_{x\in\Lambda} q^{(x,x)/2},$$

This function is a modular form of weight $n/2$.

It satisfies the identity $\theta_\Lambda(-\frac{1}{z}) = (iz)^{n/2}\theta_\Lambda(z)$

The simplest one is the Jacobi theta function: $\vartheta(z) = \sum_{n\in\mathbb{Z}} q^{n^2}$.

It is related to the Riemann zeta function via the theta function identity and the Mellin transform:

$$\frac{1}{2}\int_0^\infty (\vartheta(it) - 1)\, t^{s/2}\,\frac{dt}{t} = \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s)$$

The modular properties of theta functions play a key role in the functional equation of $\zeta(s)$ and in explaining the distribution of its nontrivial zeros near the critical line $\Re(s) = \frac{1}{2}$.

Fermat's Last Theorem

Theorem

If $p \geq 5$ *is prime, and* $a, b, c \in \mathbb{Z}$*, then*

$$a^p + b^p + c^p = 0 \quad \Rightarrow \quad abc = 0$$

- Fermat: "I have a truly marvelous proof of this proposition, which this margin is too narrow to contain."
- $n = 4$: infinite descent
- $p = 3, 5$: quadratic forms
- "regular" primes: cyclotomic extensions
- number of solutions: Faltings' theorem $\Rightarrow$ finitely many solutions
- general n: elliptic modular forms!

Reduction of Elliptic Curves

A minimal Weierstrass equation of an elliptic curve E over $\mathbb{Q}$ is of the form:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where $a_i \in \mathbb{Z}$, and the equation is minimal in the sense that the discriminant Δ has minimal valuation at each prime.

The reduction of E modulo a prime p, denoted $\widetilde{E}$, is obtained by reducing the coefficients modulo p:

$$\widetilde{E} : y^2 + \bar{a}_1xy + \bar{a}_3y = x^3 + \bar{a}_2x^2 + \bar{a}_4x + \bar{a}_6$$

At each prime p, the reduction $\widetilde{E}$ falls into one of the following types:

- **Good reduction**: $\widetilde{E}$ is a smooth curve over $\mathbb{F}_p$
- **Multiplicative reduction**:
  - *Split*: the singular point is a node with rational tangent directions
  - *Non-split*: the singular point is a node with non-rational tangents
- **Additive reduction**: the singular point is a cusp (i.e., more degenerate than a node)

Conductor

The **conductor** N_E of an elliptic curve E over $\mathbb{Q}$ is defined as:

$$N_E = \prod_{\text{primes } p} p^{f_p}$$

where f_p is given by:

$$f_p = \begin{cases} 0 & \text{if } E \text{ has good reduction at } p \\ 1 & \text{if } E \text{ has multiplicative reduction at } p \\ 2 & \text{if } E \text{ has additive reduction at } p \end{cases}$$

L-function of Elliptic Curve

Let $a_p = p + 1 - \#\widetilde{E}(\mathbb{F}_p)$ for primes p of good reduction, where $\#\widetilde{E}(\mathbb{F}_p)$ is the number of $\mathbb{F}_p$-points on the reduced curve $\widetilde{E}$.

The local zeta factor at each prime p is:

$$Z_p(T) = \begin{cases} (1 - a_p T + pT^2)^{-1} & \text{if good reduction} \\ (1 - T)^{-1} & \text{if split multiplicative reduction} \\ (1 + T)^{-1} & \text{if non-split multiplicative reduction} \\ 1 & \text{if additive reduction} \end{cases}$$

Then the **Hasse–Weil** *L*-**function** of E is:

$$L(E, s) = \prod_p Z_p(p^{-s})$$

Galois Representation of Elliptic Curves

Let E be an elliptic curve over $\mathbb{Q}$. Let

$$E[m] := \{P \in E(\overline{\mathbb{Q}}) \mid mP = 0\} \cong (\mathbb{Z}/m\mathbb{Z})^2$$

denote the group of m-torsion points on E.

The p-adic Tate module is defined as:

$$T_p(E) := \varprojlim E[p^n] \cong \mathbb{Z}_p^2$$

This gives rise to a continuous p-adic Galois representation:

$$\rho_{E,p} : G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_p)$$

which describes actions of $G_{\mathbb{Q}}$ on $T_p(E)$

The residual representation modulo p is:

$$\bar{\rho}_{E,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$$

which describes actions of $G_{\mathbb{Q}}$ on $E[p] \cong \mathbb{F}_p^2$

Moduli Spaces

The principal congruence subgroup of level N is:

$$\Gamma(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \,\middle|\, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \mod N \right\}$$

Some Hecke congruence subgroups of level N are:

$$\Gamma_0(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \,\middle|\, c \equiv 0 \mod N \right\},$$

$$\Gamma_1(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N) \,\middle|\, a \equiv d \equiv 1 \mod N \right\}$$

Let H be a congruence subgroup of $SL_2(\mathbb{Z})$. We can similarly define the complex vector space of modular forms $M_k(H)$ (resp. cusp forms $S_k(H)$) of weight k relative to H and operators on them.

A complex structure can be placed on the quotient $\Gamma \backslash \mathbb{H}$, denoted $Y(\Gamma)$.

- $Y_0(N) = Y(\Gamma_0(N))$ is the moduli space of pairs (E, C), where E is an elliptic curve and $C \subset E$ is a cyclic subgroup of order N.
- $Y_1(N)$ is the moduli space of pairs (E, P), where E is an elliptic curve and $P \in E$ is a point of order N.

Modular Curves

The compactification of $Y(\Gamma)$ is obtained by adding finitely many points called the *cusps* of Γ.

Let $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$, $\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$. Points in $\mathbb{P}^1(\mathbb{Q})$ are called *cusps*.

Two points in $\mathbb{H}^*$ are said to be Γ-equivalent if they lie in the same Γ-orbit. This defines an equivalence relation on $\mathbb{H}^*$.

The quotient space $X(\Gamma) := \Gamma \backslash \mathbb{H}^*$ is called the **modular curve** associated with Γ.

There is an explicit model for the classical modular curve $X_0(N) = X(\Gamma_0(N))$: $\Phi_N(x, y) = 0,$ such that $\Phi_N(j(N\tau), j(\tau)) = 0$.
For example,
$\Phi_2(x, y) = x^3 - x^2y^2 + 1488x^2y - 162000x^2 + 1488xy^2 + 40773375xy + 8748000000x + y^3 - 162000y^2 + 8748000000y - 157464000000000$

Hecke Operator

For a lattice $\Lambda \subset \mathbb{C}$, the Hecke operator $T(n)$ acts as:

$$T(n)F(\Lambda) = \sum_{\Lambda' \subset \Lambda,\, [\Lambda:\Lambda']=n} F(\Lambda').$$

Let the modular form $f(\tau) = F(\Lambda_\tau)$, where $\Lambda_\tau = \mathbb{Z} + \tau\mathbb{Z}$.

$$T(n)f(z) = n^{2k-1} \sum_{\substack{a\geq 1, ad=n \\ 0\leq b<d}} d^{-2k} f\left(\frac{az+b}{d}\right),$$

which is again a modular form of the same weight $2k$.
The Fourier coefficients of $f(z) = \sum_{n=1}^{\infty} a(n)q^n$ transforms as

$$T(n)f(z) = \sum_{m=1}^{\infty} \gamma(m)q^m,$$

where

$$\gamma(m) = \sum_{\substack{d|\gcd(m,n) \\ d\geq 1}} d^{2k-1}\, a\left(\frac{mn}{d^2}\right)$$

Hecke Form

A modular form $f = \sum a_n q^n$ is called a normalized Hecke eigenform if:

$$T(n)f = \lambda(n)f \quad \text{for all } n \geq 1, \quad \text{with } a_1 = 1.$$

For normalized Hecke eigenform f, $a_n = \lambda(n)$ for all $n \geq 1$.

Arithmetically, the Fourier coefficients satisfy:

- $a_n a_m = a_{nm}$ if $\gcd(n, m) = 1$,
- $a_p a_{p^n} = a_{p^{n+1}} + p^{2k-1} a_{p^{n-1}}$ for all primes p and $n \geq 1$.

Analytically, the associated L-function is:

$$L(f, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_{p \text{ prime}} \frac{1}{1 - a_p p^{-s} + p^{2k-1-2s}}$$

Petersson Inner Product

The Petersson inner product is defined by

$$\langle f, g\rangle := \int_{\mathrm{D_H}} f(\tau)\overline{g(\tau)}\,(\operatorname{Im}\tau)^{2k}\,d\nu(\tau),$$

where:

- $\mathrm{D} = \left\{\tau \in \mathbb{H} : |\operatorname{Re}\tau| \le \frac{1}{2}, |\tau| \ge 1\right\}$ is a fundamental domain for the modular group $SL_2(\mathbb{Z})$. $D_H = \cup g_i D$ where g_i are coset representatives of $SL_2(\mathbb{Z})/H$ is a fundamental domain for H.
- For $\tau = x + iy$, the hyperbolic volume form is $d\nu(\tau) = y^{-2}\,dx \wedge dy$.

properties:

- S_k is a Hilbert space.
- Self-adjointness:

$$\langle T(n)f, g\rangle = \langle f, T(n)g\rangle$$

- S_k has an orthonormal basis consisting of simultaneous eigenfunctions of all the Hecke operators. The eigenvalues of T(n) are real numbers.

Newforms

Observe that $\Gamma_0(N) \subset \Gamma_0(M)$ when $M \mid N$, so

$$S_k(\Gamma_0(M)) \subset S_k(\Gamma_0(N)).$$

The space of cusp forms of weight k and level N, denoted $S_k(\Gamma_0(N))$, admits the decomposition:

$$S_k(\Gamma_0(N)) = S_k^{\text{new}}(\Gamma_0(N)) \oplus S_k^{\text{old}}(\Gamma_0(N)) = S_k^{\text{new}}(\Gamma_0(N)) \oplus \sum_{p \mid N} S_k^{\text{old}}(\Gamma_0(N/p)).$$

- $\mathbf{S_k^{new}(\Gamma_0(N))}$: the space of **newforms** — cusp forms that are genuinely of level N, not arising from lower levels.
- $\mathbf{S_k^{old}(\Gamma_0(N))}$: the space of **oldforms** — generated by cusp forms coming from lower levels $M \mid N$ (with $M < N$), via:
  - inclusion of $S_k(\Gamma_0(M)) \hookrightarrow S_k(\Gamma_0(N))$,
  - and *degeneracy maps*$f(z) \mapsto f(dz) \quad$ for $d \mid \frac{N}{M}$,

Newforms are simultaneous eigenfunctions of all Hecke operators and form an orthonormal basis for $S_k^{\text{new}}(\Gamma_0(N))$.

Galois Representations of Newforms

The Jacobian of the modular curve is $Jac(X(\Gamma)) = S_2(\Gamma)^* \backslash H_1(X)$.
The integral Hecke algebra acting on $S_2(\Gamma_0(N))$ is

$$\mathbb{T}_{\mathbb{Z}} = \mathbb{Z}[T_n \mid n \geq 1] \subset \mathrm{End}_{\mathbb{C}}(S_2(\Gamma_0(N))).$$

Given a normalized Hecke eigenform $f \in S_2(\Gamma_0(N))$, define the ideal:

$$I_f := \ker\left(\mathbb{T}_{\mathbb{Z}} \to \mathbb{Z},\ \ T \mapsto a_n(f)\right),$$

where $a_n(f)$ is the nth Fourier coefficient of f.
The quotient ring $\mathbb{T}_{\mathbb{Z}}/I_f = \mathcal{O}_f = \mathbb{Z}[a_n(f)]$ is the ring of integers in the number field $K_f := \mathbb{Q}(a_n(f))$.
Let $A_f := J_0(N)/I_f J_0(N)$. Here $J_0(N) = Jac(X_0(N))$.
Then A_f is an abelian variety over $\mathbb{Q}$ of dimension $[K_f : \mathbb{Q}]$.
Define the p-adic Tate module: $T_p(A_f) := \varprojlim_n A_f[p^n]$ $\quad T_p(A_f) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is a free module of rank 2 over $K_f \otimes \mathbb{Q}_p$.
This yields a Galois representation:

$$\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(K_f \otimes \mathbb{Q}_p),$$

Frey Curve

For a triple of coprime integers A, B, C satisfying $A + B + C = 0$, consider the elliptic curve $E_{A,B,C}$ defined by:

$$E_{A,B,C} : \quad y^2 = x(x - A)(x + B)$$

If $a^p + b^p + c^p = 0$ with $a, b, c \in \mathbb{Z}$ and $p \geq 3$, then the associated Frey curve E_{a^p,b^p,c^p} is a semistable elliptic curve with conductor:

$$N_E = \prod_{\ell | abc} \ell$$

Without loss of generality, assume $a \equiv -1 \pmod 4$ and $2 \mid b$. Then the associated Galois representation $\bar{\rho}_{E,p}$ is:

- absolutely irreducible,
- odd (i.e. complex conjugation has determinant -1),
- unramified outside $2p$ and flat at p.

Ribet's Theorem

Theorem

Let $f \in S_2(\Gamma_0(N\ell))$ be a newform, where $\ell \nmid N$ is a prime. Suppose the associated residual Galois representation $\bar{\rho}_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$ is absolutely irreducible.

If one of the following conditions holds:

- *$\bar{\rho}_f$ is flat at $\ell = p$,*
- *or $\bar{\rho}_f$ is unramified at ℓ*

then there exists a newform $g \in S_2(\Gamma_0(N))$ such that:

$$\bar{\rho}_g \cong \bar{\rho}_f$$

Modularity Theorem

Theorem

Every elliptic curve E over $\mathbb{Q}$ is modular.

We say E is modular if any of the following equivalent conditions hold:

1. Suppose E has conductor N_E. Then there exists a newform $f \in S_2(\Gamma_0(N_E))$ such that
$$L(E, s) = L(f, s)$$
2. There exists a non-constant morphism of algebraic curves over $\mathbb{Q}$,
$$\phi : X_0(N_E) \to E$$
3. For some (equivalently, for all) primes p, there exists a newform $f \in S_2(\Gamma_0(N_E))$ such that:
$$\rho_{E,p} \cong \rho_{f,p}$$

- (1) $\Leftrightarrow$ (2) via the Eichler–Shimura relations.
- (1) $\Leftrightarrow$ (3) via properties of the Frobenius element.

Proof of Fermat's Last Theorem

Sketch of Proof.

Assume, for contradiction, that there exists a nontrivial solution $a^p + b^p + c^p = 0$.
Let E_{a^p,b^p,c^p} be the associated Frey curve. with conductor N_E.
By the modularity theorem , E_{a^p,b^p,c^p} is modular:

$$\exists f \in S_2(\Gamma_0(N_E)) \quad \text{such that} \quad \rho_f \cong \rho_E$$

The associated residual Galois representation $\bar{\rho}_E$ is absolutely irreducible, unramified outside $2p$, flat at p.
By Ribet's theorem, it follows that:

$$\exists g \in S_2(\Gamma_0(2)) \quad \text{such that} \quad \bar{\rho}_g \cong \bar{\rho}_f$$

However, $\dim S_2(\Gamma_0(2)) = 0$, since the genus of the modular curve $X_0(2)$ is zero. Hence, no such form g exists — a contradiction. □

Siegel Modular Forms

The **Siegel modular group** of genus g is the symplectic group:

$$\mathrm{Sp}_{2g}(\mathbb{Z}) = \left\{ \gamma \in \mathrm{GL}_{2g}(\mathbb{Z}) \,\middle|\, \gamma^T J \gamma = J \right\}, \quad J = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}$$

The **Siegel upper half-plane** of genus g is:

$$\mathbb{H}_g = \left\{ \tau \in \mathrm{Mat}_{g\times g}(\mathbb{C}) \,\middle|\, \tau^T = \tau,\ \mathrm{Im}(\tau) > 0 \right\}$$

A **Siegel modular form** of weight ρ (a representation) is a holomorphic map $f : \mathbb{H}_g \to V \simeq \mathbb{C}^n$ if:

$$f(\gamma \cdot \tau) = \rho(c\tau + d) \cdot f(\tau) \quad \text{for all } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sp}_{2g}(\mathbb{Z}),\ \tau \in \mathbb{H}_g$$

Applications:

- Their Hecke eigenvalues correspond to Satake parameters for $\mathrm{GSp}_{2g}(\mathbb{Q}_p)$. Local Hecke algebra $\mathcal{H}_l = \mathcal{H}(\mathrm{GSp}_{2g}(\mathbb{Q}_l), \mathrm{GSp}_{2g}(\mathbb{Z}_l))$
- **Satake isomorphism**

$$\bar{\mathbb{F}}_p \otimes \mathcal{H}_l \xrightarrow{\sim} \bar{\mathbb{F}}_p \otimes \mathrm{Representation}(\mathrm{GSp}_{2g}^{\mathrm{dual}})$$

Conclusion & Future Work

$$\rho : G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_n$$

- $n = 1$: **class field theory**
- $n = 2$: **elliptic modular forms**
- general n: Your Homework!

Thank you!