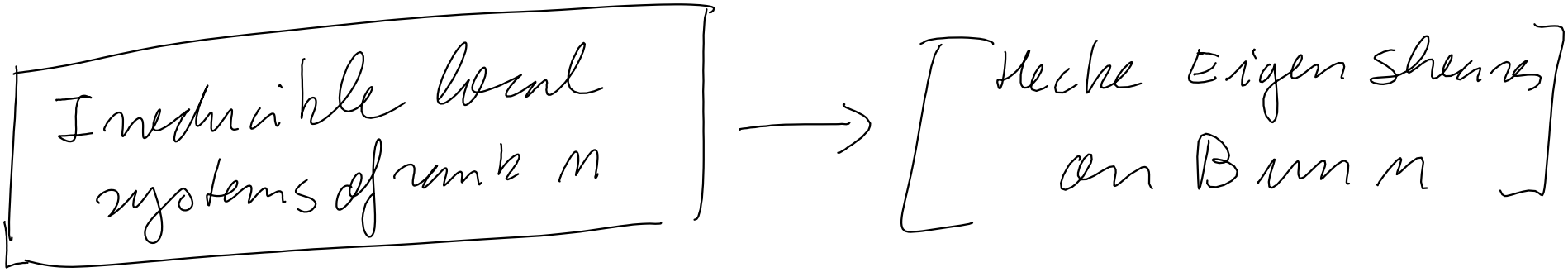
An introduction to Hecke correspondences and the modularity theorem.

Madrid, October 16 2009

Referencia: Diamond, F., Shurman, J., A first course in modular forms GTM 228. Springer Verlag 2005.

- Geometric Langlands conjecture for GL_n

X a curve : There is a correspondence



$$E \longmapsto Aut_E$$

Such that Aut_E is an E-eigensheaf.

Langlands conjecture for number fields

F a number field. There is a correspondence

$$\boxed{n\text{-dim reps of } \mathrm{Gal}(\bar{F}/F)} \longrightarrow \boxed{\text{cuspidal automorphic reps. of } GL_n(\mathbb{A}_F)}$$

Such that

$$\text{Frobenius eigenvalues} \longmapsto \text{Hecke eigenvalues}$$

Case $n = 2$

- Cuspidal automorphic representations give rise to classical modular forms.

- Hecke operators are the classical Hecke operators

- When $F = \mathbb{Q}$ and we start with the Galois rep. associated to an elliptic curve over $\mathbb{Q}$, we obtain Taniyama - Shimura - Weil conjecture that implies Fermat's last theorem.

① Modular forms:

$\mathbb{H} = \{z = x+iy \mid y>0\}$ Poincaré half-plane.

$SL_2(\mathbb{R})$ acts on $\mathbb{H}$ by Möbius transform:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}$$

Modular group $\Gamma = SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid \begin{matrix} a,b,c,d \in \mathbb{Z} \\ ad-bc=1 \end{matrix} \right\}$

A meromorphic function $f: \mathbb{H} \to \mathbb{C}$ is weakly modular of weight k (with respect to Γ) if

$$f(\gamma \cdot z) = (cz+d)^k f(z) \qquad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

- Consider $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma$, then $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot z = z+1$ so f is periodic

- The Fourier development: $q = e^{2\pi i z}$:

$$f(z) = \sum_{n \in \mathbb{Z}} a_n q^n$$

A modular form of weight k (with respect to Γ) is a function $f: \mathbb{H} \to \mathbb{C}$ such that

1) f is holomorphic in $\mathbb{H}$
2) f is weakly modular of weight k.
3) $a_n = 0 \ \forall n < 0$ (holomorphic at ∞)

} $M_k(\Gamma)$

If $a_0 = 0$ we say that f is cuspidal $S_k(\Gamma)$

- Geometric interpretation:
  - $Y = Y(1) = \Gamma \backslash \mathbb{H}$ is the set of complex points of the "coarse" moduli space of elliptic curves: Modular curve
  - $X = X(1) = X \amalg \{\infty\} \cong \mathbb{P}^1(\mathbb{C})$: Compactified modular curve.
  - $M_{12k}(\Gamma) \cong \Gamma(\mathbb{P}^1, \mathcal{O}(k))$; $S_{12k}(\Gamma) \cong \Gamma(\mathbb{P}^1, \mathcal{O}(k-1))$

Original of 12: $-\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in SL_2(\mathbb{Z}) \Rightarrow M_{2k+1}(\Gamma) = 0$

- there are elliptic points of order 2 and 3

So $M_k(\Gamma)$ are associated to rational divisors.

Congruence subgroups:

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

A **congruence subgroup** is a subgroup of Γ that contains a $\Gamma(N)$:

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod N \right\}$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod N \right\}$$

$$\Gamma_1^0(N,p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & 0 \\ * & * \end{pmatrix} \bmod p, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod N \right\}$$

From the congruence subgroups we obtain more modular curves.

$$Y_0(N) = \Gamma_0(N)\backslash\mathbb{H} = \left\{ (E, C) \;\middle|\; \begin{array}{l} E \text{ elliptic curve} \\ C \text{ cyclic subgroup} \\ \text{order } N \end{array} \right\} / \cong$$

$$Y_1(N) = \Gamma_1(N)\backslash\mathbb{H} = \left\{ (E, Q) \;\middle|\; \begin{array}{l} E \text{ elliptic curve} \\ Q \text{ a point of order } N \end{array} \right\} / \cong$$

$$Y_1^0(N,P) = \Gamma_1^0(N)\backslash\mathbb{H} = \left\{ (E, C, Q) \;\middle|\; \begin{array}{l} E \text{ elliptic curve} \\ C \text{ cyclic subgroup order } p \\ Q \text{ point of order } N \\ \langle Q \rangle \cap C = \{0\} \end{array} \right\} / \cong$$

* The definition of weakly modular can be extended to any congruence subgroup Γ':

$$f(\gamma . z) = (cz+d)^{2} f(z) \quad \forall \gamma \in \Gamma'$$

* We can compactify the modular curves adding a finite number of cusps: For any congruence subgroup $\Gamma(N) \subseteq \Gamma' \subseteq \Gamma$

$$Y(\Gamma') = \Gamma' \backslash \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$$

If $[c] \in \Gamma' \backslash \mathbb{P}^1(\mathbb{Q})$ is a cusp for Γ', $\exists\, \alpha \in SL_2(\mathbb{Q})$

s.t. $\alpha . c = \infty$.

There is an $h \geq 1$ minimal such that

$$\alpha \cdot \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \cdot \alpha^{-1} \in \Gamma'$$

It generates the parabolic subgroup fixing c.

If f is weakly modular with respect to Γ'

the Fourier expansion of f at c is the Fourier

expansion

$$f(\alpha^{-1} z) = \sum_{n \in \mathbb{Z}} a_n q^n \qquad q = e^{2\pi i z/h}.$$

A **Modular form** with respect to Γ' is a function

$$f : \mathcal{H} \to \mathbb{C} \quad \text{such that}$$

1) f has to be holomorphic
2) f is weakly modular w.r. Γ'
3) For each cusp $c \in \rho^{-1}(\mathbb{P}^1(\mathbb{Q}))$ the Fourier expansion of f at c: $f = \sum_{n \in \mathbb{Z}} a_n q^n$ satisfies $a_n = 0 \ \forall n < 0$

It is cuspidal if moreover $a_0 = 0$.

Space of modular forms $M_k(\Gamma')$

Space of cuspidal modular forms $S_k(\Gamma')$.

If we forget the problems related with elliptic points, we can identify the elements of $M_k(\Gamma')$ and $S_k(\Gamma')$ with sections of line bundles on $X(\Gamma')$.

Basic example! There is an isomorphism

$$\omega : S_2(\Gamma') \longrightarrow \Omega^1(X(\Gamma'))$$

We can identify cuspidal weight 2 modular forms with differentials.

- Consider $\Gamma_1(N)$, $N \geq 4$: $Y_1(N)$ is a fine moduli space
- $E(N) \to Y_1(N)$ universal family; $\bar{E}(N) \to X_1(N)$
- $\Omega^1_{\bar{E}(N)/X_1(N)}$ relative cotangent bundle.
- $\varepsilon : X_1(N) \to \bar{E}(N)$ the zero section.

Then:

$$M_k(\Gamma_1(N)) = \Gamma\left(X_1(N), \left(\varepsilon^* \Omega^1_{\bar{E}(N)/X_1(N)}\right)^{\otimes k}\right)$$

Maps between modular curves and modular forms

If we have two congruence subgroups $\Gamma_1 \subseteq \Gamma_2$

we have the natural inclusion $M_k(\Gamma_2) \subseteq M_k(\Gamma_1)$

and the trace map $M_k(\Gamma_1) \to M_k(\Gamma_2)$

$$f \longmapsto t_2(f)(z) = \sum_{\bar{\gamma} \in \Gamma_1 \backslash \Gamma_2} (cz+d)^k f(\gamma z)$$

Geometrically this corresponds to the inverse and the direct image with respect to

$$X(\Gamma_1) \to\!\!\to X(\Gamma_2).$$

If Γ_1 is a congruence subgroup and $\alpha \in GL_2^+(\mathbb{Q})$ such that $\Gamma_1' = \alpha \Gamma_1 \alpha^{-1}$ is a congruence subgroup.

Then we have isomorphisms translation by α

$$M_k(\Gamma_1) \longrightarrow M_k(\Gamma_1')$$

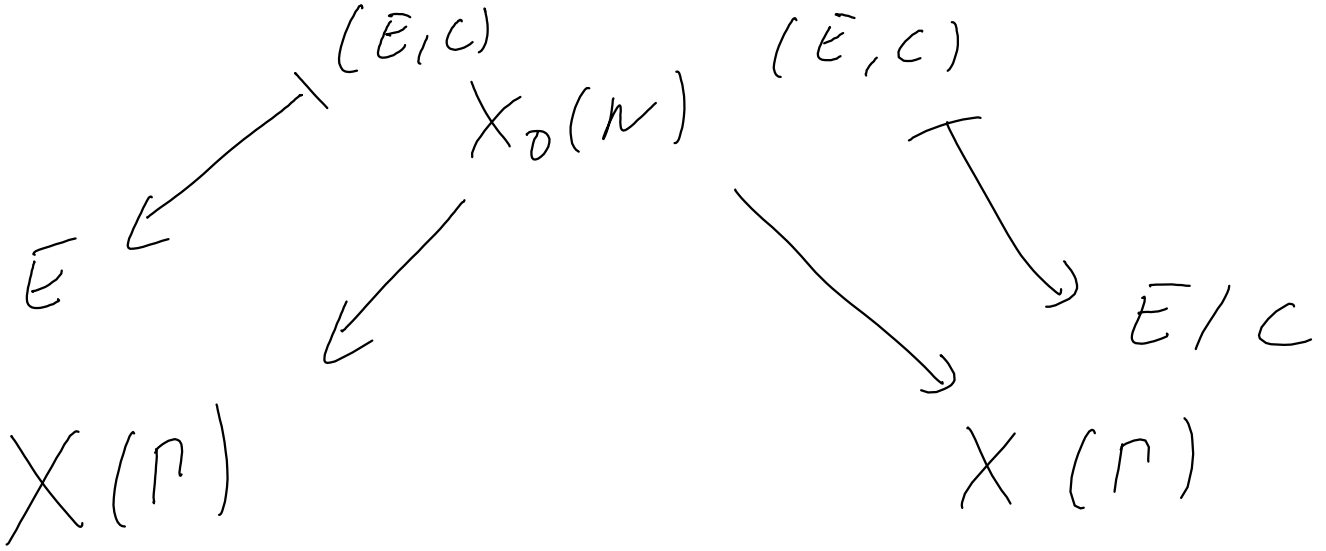
$$f \longmapsto f[\alpha]_k : z \mapsto (\det \alpha)^{k-1} (cz+d)^{-k} f(\alpha z)$$

$$\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

and an isomorphism

$$X(\Gamma_1') \longrightarrow X(\Gamma_1)$$

Example: We want to interpret, in terms of groups, the correspondence



This diagram corresponds to

$$\begin{array}{ccc} \Gamma_0(N) & \xrightarrow{\sim} & \Gamma_0'(N) = \begin{pmatrix} 1 & 0 \\ 0 & N \end{pmatrix}^{-1} \Gamma_0(N) \begin{pmatrix} 1 & 0 \\ 0 & N \end{pmatrix} = \left\{ \begin{pmatrix} * & 0 \\ * & * \end{pmatrix} \bmod N \right\} \\ \cap | & & \cap | \\ \Gamma & & \Gamma \end{array}$$

Interesting maps between modular curves:

- $Y_1(N) \xrightarrow{\pi} Y_0(N)$: $\Gamma_1(N) \subseteq \Gamma_0(N)$

  $(E, Q) \mapsto (E, \langle Q \rangle)$

- Diamond operator

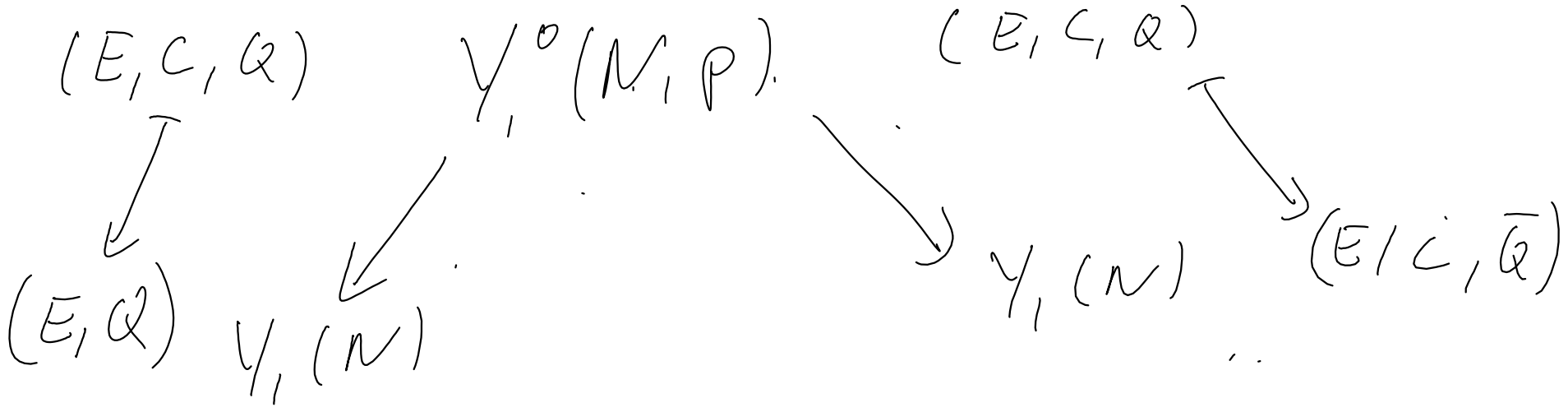
  if $(d, N) = 1$ $\quad \langle d \rangle : Y_1(N) \to Y_1(N)$

  $= \quad (E, Q) \mapsto (E, d \cdot Q)$

if $\alpha = \begin{pmatrix} * & * \\ * & d \end{pmatrix} \in \Gamma_0(N)$ then $\alpha \, \Gamma_1(N) \, \alpha^{-1} = \Gamma_1(N)$

The map $\langle d \rangle$ is the translation by α.

The Hecke correspondence p prime with N



At the level of groups is give by

$$\Gamma_1^0(N,p) \xrightarrow{\simeq} \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma_1^0(N,p) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}^{-1}$$

$$\downarrow \qquad\qquad \downarrow$$

$$\Gamma_1(N) \qquad\qquad \Gamma_1(N)$$

Proposition: - The Hecke operators T_p and the diamond operators $\langle d \rangle$ commute with each other. Moreover they are normal with respect to the Petersson inner product of $S_k(N)$.

The Hecke algebra of level N and weight k is the algebra of operators

$$\mathbb{T}_k = \mathbb{T}_k(N) = \mathbb{Z}\{T_p, \langle d \rangle\}$$

It is a finitely generated commutative algebra.

Notation:

- $M_k(N) = M_k(\Gamma_0(N))$, $S_k(N) = S_k(\Gamma_0(N))$

- Let $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$ a character

$$M_k(N, \chi) = \{ f \in M_k(\Gamma_1(N)) \mid \langle d \rangle f = \chi(d) \cdot f \}$$

Then

$$M_k(\Gamma_1(N)) = \bigoplus_\chi M_k(N, \chi)$$

$$M_k(N) = M_k(N, 1)$$

Description of the space of modular forms

- The Eisenstein series provide explicit modular forms.
- Let $\mathcal{E}_k(N, \chi)$ the space of modular forms that can be obtained as Eisenstein series. Then

$$M_k(N, \chi) = \mathcal{E}_k(N, \chi) \oplus S_k(N, \chi)$$

To describe $M_k(N, \chi)$ is "enough" to describe $S_k(N, \chi)$.

New-forms and Old forms.

* If $N \mid M$ then $S_k(\Gamma_1(N)) \subseteq S_k(\Gamma_1(M))$.
* Moreover if $d \cdot N = M$ $\quad S_k(\Gamma_1(N)) \xrightarrow{i_d} S_k(\Gamma_1(M))$

$$f(z) \longmapsto f(dz)$$

Then $$S_k(\Gamma_1(N))^{old} = \sum_{\substack{p \mid N \\ p \text{ prime}}} S_k(\Gamma_1(Np^{-1})) + S_k(\Gamma_1(Np^{-1}))$$

$S_k(\Gamma_1(N))^{new}$ is the orthogonal complement to $S_k(\Gamma_1(N))^{old}$ w.r.t. the Petersson product

The Hecke algebra respects this decomposition.

Eigen forms

Definition: a form $f \in M_k(\Gamma_1(N))$ is a **eigen form** if it is a eigenvector of all T_p and $\langle d \rangle$. It is **normalized** if $a_1(f) = 1$. It is a **new form** if moreover $f \in S_k(\Gamma_1(N))^{new}$.

The new forms form an orthogonal basis of $S_k(\Gamma_1(N))^{new}$. Moreover

$$T_p(f) = a_p(f) \cdot f$$

Theorem

$$\mathcal{B}_k(N) = \left\{ f(mz) \;\middle|\; f \text{ a new form of level } M,\ m \cdot M \mid N \right\}$$

is a basis of $S_k(\Gamma_1(N))$

Proposition: $f \in M_k(N, \chi)$ is a normalized eigen form if

1). $a_1(f) = 1$

2) $a_{p^r}(f) = a_p(f) \cdot a_{p^{r-1}}(f) - \chi(p) p^{k-1} a_{p^{r-2}}(f)$

3) $a_{mn}(f) = a_m(f) \cdot a_n(f)$ if $(m, n) = 1$.

L-Series

If $f \in M_k(\Gamma_1(N))$; $f = \sum a_n(f)\, q^n$

The Dirichlet series is $s \in \mathbb{C}$

$$L(f,s) = \sum \frac{a_n(f)}{n^s}$$

Theorem: The series converges for $Re(s) > k$ and if f is a cusp form it converges for $Re(s) > k/2 + 1$

Theorem $f \in M_k(N, \chi)$ is a normalized eigen form if and only if $L(f,s)$ has an Euler product

$$L(f,s) = \prod_{p \text{ primo}} \left(1 - a_p p^{-s} + \chi(p) p^{k-1-2s}\right)^{-1}$$

Theorem: If f is a cusp form then $L(f,s)$ can be extended to a entire function on the whole plane that satisfies a functional equation

Elliptic curves

E elliptic curve / $\mathbb{Q}$ in reduced form

N_E conductor: measures the primes of bad reduction and the type of reduction

counting function: $a_p(E) = p + 1 - \#\tilde{E}(\mathbb{F}_p)$

$$L(E,s) = \prod_{p \nmid N_E} \frac{1}{(1 - a_p(E)\, p^{-s} + p^{-2s+1})} \cdot \prod_{p \mid N_E} \quad *$$

the Hasse-Weil L-function of E.

- Can be extended to an entire function?
- Functional equation?

Galois representations

Fix ℓ a prime.

Tate module: $T_\ell(E) = \varprojlim_n E(\bar{\mathbb{Q}})[\ell^n] \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$

It carries a $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ representation: ρ

If $p \nmid \ell, N_E$ then ρ is unramified at p.

So Frob_p acts on $T_\ell(E)$

Theorem: $\mathrm{tr}(\mathrm{Frob}_p) = a_p(E)$

Langlands correspondence:

predicts:

$\rho_E, \{\operatorname{tr} \mathrm{Frob}_p\} \longrightarrow$ f new form

$\{a_p(E)\}$ $\{$eigenvalues of Hecke$\}$

$\Downarrow$ $\{a_p(f)\}$

$$L(E,s) = L(f,s)$$

$\Rightarrow$ analytic extension and functional equation for $L(E,s)$

Modularity theorem

Wiles - Breuil - Conrad - Diamond - Taylor

Version 1: E elliptic curve over $\mathbb{Q}$. then there exist a new form $f \in S_2(\Gamma_0(N_E))^{\text{new}}$ such that

$$L(E,s) = L(f,s)$$

Version 2: E elliptic curve over $\mathbb{Q}$, then there exists a surjective morphism over $\mathbb{Q}$

$$X_0(N_E) \longrightarrow E.$$

Famous consequences

1) Fermat's last Theorem..

2) Gross-Zagier-Kolyvagin proof of rank 1 case of BSD conjecture is valid for all