Paper due at 1 pm, August 31

(email to me).

Last time

Prop

Let $E/\mathbb{Q}$ be an ell. curve of conductor N.

(1) $\{V_\ell E\}$ forms a compatible system of ℓ-adic rep'ns

(2) For $p \nmid N$, the local L-factor of the corresponding L-function is

$$\frac{1}{1 - a_p T + pT^2}$$

where $a_p = 1 + p - \# \bar{E}(\mathbb{F}_p)$

(3) $|a_p| \leq 2p^{1/2}$.

$$L(E,s) = \sum_{n \geq 1} a_n n^{-s} \quad \text{with } a_p = 1 + p - \#\bar{E}(\mathbb{F}_p) \text{ for } p \nmid N$$

$$= (*) \prod_{p \nmid N} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}.$$

Using part (3) of the prop, can show that

$L(E,s)$ converges on $\mathrm{Re}(s) > 3/2$.

Things we don't know about $L(E,s)$:

- Analytic continuation to $\mathbb{C}$
- Functional equation.

Since $E/\mathbb{Q}$, these are true. The only method we have of proving this is by showing $L(E,s) = L(f,s)$ for some $f \in S_2(\Gamma_0(N))$.

<u>Recall</u> Let $f \in S_{2k}(\Gamma_0(N))$ be a cusp form,

$$f = \sum_{n \geq 1} a_n q^n.$$

$$L(f,s) = \sum_{n \geq 1} a_n n^{-s}.$$

<u>Prop</u> For some $C > 0$, $|a_n| \leq C n^k \quad \forall n \geq 1$.

<u>Pf.</u> For any $y \in \mathbb{R}_{>0}$,

$$\int_0^1 e^{-2\pi i n(x+iy)} f(x+iy)\, dx = \int_0^1 e^{-2\pi i n(x+iy)} \sum_{m \geq 1} a_m e^{2\pi i m(x+iy)}\, dx$$

$$= \int_0^1 \sum_{m \geq 1} a_m e^{2\pi i (m-n)(x+iy)}\, dx$$

$$= a_n.$$

Also we've seen $|f(\tau)|\,\mathrm{Im}(\tau)^k$ is $\Gamma_0(N)$-invariant and bounded as a function on $\mathcal{H}$.

Hence $|f(\tau)| \le C\,\mathrm{Im}(\tau)^{-k}$ some $C>0$.

$$|a_n| \le \int_0^1 \left|e^{-2\pi i n(x+iy)} f(x+iy)\right| dx \le C\int_0^1 e^{2\pi n y}\, y^{-k}\, dx = Ce^{2\pi n y} y^{-k}$$

$\forall y>0$. Setting $y = 1/n$,

$$|a_n| \le Ce^{2\pi} n^k. \qquad \square$$

<u>Cor</u> $L(f,s)$ converges on $\mathrm{Re}(s) > 1+k$.

<u>Pf.</u>

$$|L(f,s)| \le \sum_{n\ge1} |a_n n^{-s}| \le C\sum_{n\ge 1} n^{k-\mathrm{Re}(s)}$$

converges when $k - \mathrm{Re}(s) < -1$

$\iff \mathrm{Re}(s) > 1+k$. $\square$

<u>Thm</u> If $f\in S_{2k}(SL_2(\mathbb{Z}))$ then

(1) $L(f,s)$ has an analytic continuation to $\mathbb{C}$

(2) $\Lambda(f,s) = (2\pi)^{-s}\,\Gamma(s)\,L(f,s)$ satisfies

$$\Lambda(f,2k-s) = (-1)^k\,\Lambda(f,s).$$

Pf. For $\mathrm{Re}(s) > 1+k$

$$\int_0^\infty t^s f(it)\frac{dt}{t} = \int_0^\infty t^{s-1}\sum_{n\geq 1} a_n e^{-2\pi n t}\,dt$$

$$= \sum_{n\geq 1} a_n \int_0^\infty t^{s-1} e^{-2\pi n t}\,dt \qquad \Gamma(s) = \int_0^\infty u^{s-1}e^{-u}du$$

$$\begin{pmatrix} u = 2\pi n t \\ du = 2\pi n\, dt \end{pmatrix} \qquad = \sum_{n\geq 1} a_n (2\pi n)^{-s}\int_0^\infty u^{s-1}e^{-u}du$$

$$= \Gamma(s)(2\pi)^{-s}\sum_{n\geq 1} a_n n^{-s}$$

$$= \Lambda(f,s).$$

Since $\frac{(2\pi)^s}{\Gamma(s)}$ is holomorphic on $\mathbb{C}$, it suffices

to show $\Lambda(f,s)$ has an analytic cont. to $\mathbb{C}$.

$$\Lambda(f,s) = \int_0^\infty t^s f(it)\frac{dt}{t} = \int_0^1 t^s f(it)\frac{dt}{t} + \int_1^\infty t^s f(it)\frac{dt}{t}$$

$$\begin{pmatrix} u = 1/t \\ \frac{du}{u} = -\frac{dt}{t} \end{pmatrix} \qquad = \int_1^\infty \left(\frac{1}{u}\right)^s f\left(\frac{i}{u}\right)\frac{du}{u} + \int_1^\infty t^s f(it)\frac{dt}{t}$$

$$= \int_1^\infty \left(\frac{1}{u}\right)^s (iu)^{2k} f(iu)\frac{du}{u} + \underline{\qquad\qquad}$$

$$\begin{pmatrix} \frac{i}{u} = S(iu) \\ S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \end{pmatrix} \qquad = \int_1^\infty \left(t^{2k-s}(-1)^k + t^s\right) f(it)\frac{dt}{t}.$$

$f(it)$ decays exponentially as $t \to \infty$, so this integral converges for any $s \in \mathbb{C}$. This gives an analytic cont. to $\mathbb{C}$!

Also, $t^{2k-s}(-1)^k + t^s$ is $(-1)^k$-invariant under $s \longmapsto 2k-s$, giving the functional eqn. $\square$

<u>Rmk</u> The thm remains true on $\Gamma_0(N)$, but

$S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ is replaced w/ a different involution

and need to consider $f \in S_{2k}(\Gamma_0(N))^{\pm}$ ← eigenspace of the involution.

<u>Oops, I forgot to tell you about</u> Hecke operators T_p for $p|N$. They're defined in basically the same way, but the formulas are a little different.

Still self-adjoint under Petersson inner product and commute with all T_n's.

<u>Thm</u> Let $f = \sum_{n \geq 1} a_n q^n \in S_{2k}(\Gamma_0(N))$ be a normalized eigenform for all T_n.

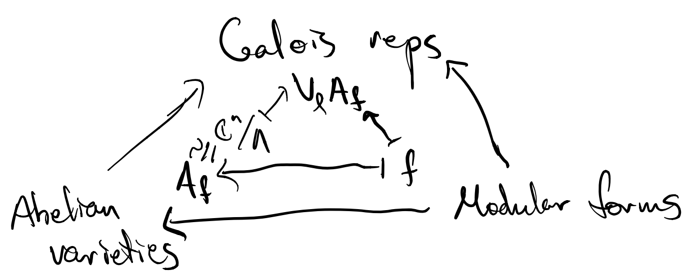
(1) all a_n are algebraic integers, and $[\mathbb{Q}(a_n) : \mathbb{Q}] < \infty$.

(2) $T_p f = a_p f \quad \forall p$ prime.

(3) $$L(f,s) = \prod_p \frac{1}{1 - a_p p^{-s} + p^{2k-1-2s}}.$$

<u>Rmk</u> Given such a f, there is a compatible system of ℓ-adic reps $\{\rho_{f,\ell}\}$ which gives the above L-function.

Where does $\rho_{f,\ell}$ come from?



<u>Thm</u> (Modularity)

Let $E/\mathbb{Q}$ be an ell. curve w/ conductor N. Then there is a normalized eigenform $f \in S_2(\Gamma_0(N))$ s.t. $L(E,s) = L(f,s)$.

In particular, $L(E,s)$ has an analytic continuation and functional equation.

<u>Defn</u> An elliptic curve is <u>modular</u> if $L(E,s) = L(f,s)$ for some f.

(So the thm says that every $E/\mathbb{Q}$ is modular.)

Defn A compatible system $\{\rho_\ell\}$ of ℓ-adic Galois reps is *modular* if

$$\rho_\ell \cong \rho_{f,\ell} \quad \forall \ell$$

for some normalized eigenform $f \in S_{2k}(\Gamma_0(N))$.

(So the thm says that $\{\rho_{E,\ell}\}$ is modular for $E/\mathbb{Q}$.)

There is also a geometric way of stating the modularity thm.

Thm (Modularity) If $E/\mathbb{Q}$ is an ell. curve of conductor N then there is a surjective map of R.S.'s

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

This map is called a *modular parametrization*.

Relation to Fermat's Last Thm

Thm (FLT) $\forall n \geq 3$, if $a,b,c \in \mathbb{Z}$ s.t.

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

then $abc = 0$.

Rmk It suffices to prove FLT in the case $n = \ell$, a prime, and $n = 4$.

Easy to prove for $n = 3, 4$, so can take $n = \ell \geq 5$.

Supposing we have a counterexample (a, b, c), Frey proposed looking at

$$E: \quad y^2 = x(x - a^\ell)(x - b^\ell) \qquad \text{(Frey curve.)}$$

E has many, many remarkable properties.

Serre showed that if the ε-conjecture is true, then E is not modular. Ribet proved the ε-conjecture.

Wiles + Taylor - Wiles proved the Modularity Theorem, and thereby FLT.