Galois Representations.

$\overline{\mathbb{Q}}$ = algebraic closure of $\mathbb{Q}$.

$G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

F a ~~nth~~ number field, $G_F = \mathrm{Gal}(\overline{F}/F)$.

Galois representation = representation of $G_{\mathbb{Q}}$ or G_F.

Fix $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p \rightsquigarrow$

$$\begin{array}{c} \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \longrightarrow G_{\mathbb{Q}} \\ \| \\ G_{\mathbb{Q}_p} \end{array}$$

decomposition group at p.

Given a representation

$$\rho : G_{\mathbb{Q}} \longrightarrow GL_n(K),$$

restriction gives $\rho|_{G_{\mathbb{Q}_p}} : G_{\mathbb{Q}_p} \to GL_n(K)$

<u>Aim</u>: study such representations of $G_{\mathbb{Q}}$, and their restrictions to the $G_{\mathbb{Q}_p}$.

<u>Example</u>

Fix $p > 2$ prime.

$\mathbb{Q}(\sqrt{p})/\mathbb{Q}$. Ramified at p, and possibly at 2.

$$\chi : G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\sqrt{p})/\mathbb{Q}).$$

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{p})/\mathbb{Q}) \cong \{\pm 1\}.$$

$$\chi : G_{\mathbb{Q}} \to \{\pm 1\}.$$

Take $\ell \neq 2, p$. Then $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$ is unramified at ℓ.

Then we have a canonical element $\mathrm{Frob}_\ell \in \mathrm{Gal}(\mathbb{Q}(\sqrt{p})/\mathbb{Q})$, lifting the mod ℓ Frobenius.

$\chi(\mathrm{Frob}_\ell) = \pm 1$. When is it $+1$?

$\chi(\mathrm{Frob}_\ell) = 1 \iff \mathrm{Frob}_\ell(\sqrt{p}) = \sqrt{p}$

$\iff (\sqrt{p})^\ell = \sqrt{p}$ in $\overline{\mathbb{F}_\ell}$

$\iff \sqrt{p} \in \mathbb{F}_\ell$

$\iff p$ is a quadratic residue mod ℓ.

i.e. $\chi(\mathrm{Frob}_\ell) = \left(\frac{p}{\ell}\right)$.

<u>Assume</u> $p \equiv 1 \pmod 4$. Then $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$ is only ramified at p, and it's the unique quadratic field with this property.

$\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is also ramified only at p.

primitive pth root of 1

$\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is Galois, with Galois gp

$$\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$$

$$(\zeta_p \mapsto \zeta_p^a) \longleftrightarrow a \pmod{p}.$$

In particular, this is cyclic of even order, so $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ contains a quadratic field only ramified at p i.e. $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta_p)$.

$$\begin{tikzcd}
\chi : G_{\mathbb{Q}} \arrow[r] & \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \arrow[r] \arrow[d, phantom, "\wr"] & \mathrm{Gal}(\mathbb{Q}(\sqrt{p})/\mathbb{Q}) \arrow[d, phantom, "\wr"] \\
 & (\mathbb{Z}/p\mathbb{Z})^\times \arrow[r] & \{\pm 1\}.
\end{tikzcd}$$

So $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic, so χ is the unique non-trivial quadratic character of $(\mathbb{Z}/p\mathbb{Z})^\times$, and the kernel of χ is just the quadratic residues in $(\mathbb{Z}/p\mathbb{Z})^\times$.

$$\mathrm{Frob}_\ell(\zeta_p) = \zeta_p^\ell$$

So $\mathrm{Frob}_\ell \mapsto \ell \bmod p \in (\mathbb{Z}/p\mathbb{Z})^\times$

$\chi(\mathrm{Frob}_\ell) = 1 \iff \ell$ is a quadratic residue mod p.

i.e. $\chi(\mathrm{Frob}_\ell) = \left(\frac{\ell}{p}\right)$.

So $\left(\frac{p}{\ell}\right) = \chi(\mathrm{Frob}_\ell) = \left(\frac{\ell}{p}\right)$.

Exercise prove the rest of quadratic reciprocity in this way.

Aim generalise this.

Started with a Galois representation, and observed that it encoded arithmetic information.

Then computed the local information in terms of something else.

e.g. $f = q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2$

$q = e^{2\pi i z}$ eigenform wt 2, level $\Gamma_0(11)$.

$$= q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} - 2q^{12} + 4q^{13} + \dots a_n q^n + \dots$$

$E : y^2 + y = x^3 - x^2$

p	2	3	5	7	13	17 ...
$\#E(\mathbb{F}_p)$	4	4	4	9	9	19
$p - \#E(\mathbb{F}_p)$	-2	-1	1	-2	4	-2

Coefficients in the q-expansion.

E is <u>modular</u>, corresponding to f.

Where is the Galois representation?

Answer: use the action of $G_{\mathbb{Q}}$ on torsion points of E.

For any $N \geq 1$, let $E[N] =$
$\{N\text{-torsion points of } E\}$

$E[N] \simeq (\mathbb{Z}/N\mathbb{Z})^2$ as an abelian group

The coordinates of points in $E[N]$ are in $\overline{\mathbb{Q}}$, so $G_{\mathbb{Q}} \circlearrowright E[N]$

i.e. $\rho_E : G_{\mathbb{Q}} \to GL_2(\mathbb{Z}/N\mathbb{Z})$

<u>Fact</u> If $\ell \nmid 11N$ then ρ_E is unramified at ℓ, and

$$\operatorname{tr} \rho_E(\mathrm{Frob}_\ell) = a_\ell \pmod{N}.$$

f is determined by the a_ℓ

ρ_E is determined up to isomorphism by $\operatorname{tr} \rho_E(\mathrm{Frob}_\ell)$ [uses $\{\mathrm{Frob}_\ell\}_{\ell \neq 11}$ are dense in $G_{\mathbb{Q}}$ $\leftarrow$ Chebotarev].

Consider all of these representations

$$\rho_E : G_{\mathbb{Q}} \to GL_2(\mathbb{Z}/N\mathbb{Z}) \text{ at once.}$$

By CRT, enough to consider $N = p^r$, $r \geq 1$.

Then the representations compile together to give

$$\rho_{E,p} : G_{\mathbb{Q}} \longrightarrow GL_2(\varprojlim \mathbb{Z}/p^r\mathbb{Z})$$
$$= GL_2(\mathbb{Z}_p).$$

Continuous w.r.t. natural topologies: profinite topology on $G_{\mathbb{Q}}$, and p-adic topology on $GL_2(\mathbb{Z}_p)$.

Consider all of the $\rho_{E,p}$ as p varies: get a <u>compatible system</u> or <u>compatible family</u> of Galois representations

$$\rho_{E,p} : G_{\mathbb{Q}} \to GL_2(\mathbb{Z}_p):$$

<u>compatible</u>: $\exists$ common ramification set $\{11\}$, in the sense that if $\ell \neq 11, p$ then $\rho_{E,p}$ is unramified at ℓ, and

$\mathrm{tr}\, \rho_{E,p}(\mathrm{Frob}_\ell)$ is independent of $p \neq 11, \ell$

In particular, $\mathrm{tr}\, \rho_{E,p}(\mathrm{Frob}_\ell) \in \mathbb{Z}$.

The property of being in a compatible system is restrictive: conjecturally, it implies that the representation "come from geometry" + "come from automorphic forms".

Aim of modularity lifting theorems: show that Galois representations do indeed come from automorphic forms.

[+ in some cases, then deduce that they come from geometry].