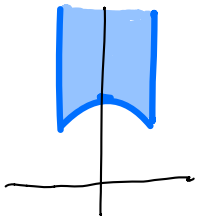
2021

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

arizona



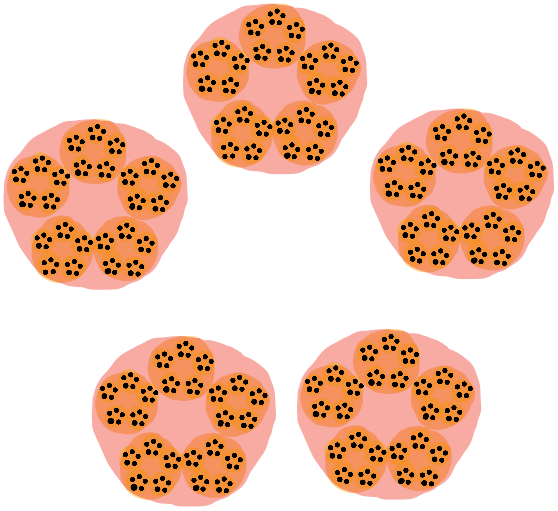
inter

p-adic Lecture 6: p-aradigm shift

Sch??l

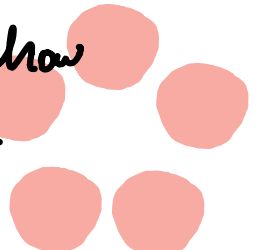
5.1 Inverse Limit Mathematics

- The marvelous proof of Fermat's Last Theorem will not fit into the margins of this lecture...

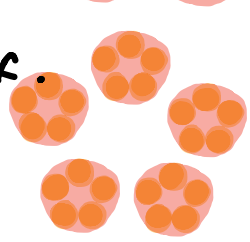


- Leci n'est pas $\mathbb{Z}_p$

1) Paint one layer on with the mod p approx, see how the big chunks fit together



2) Add another layer: $\mathbb{Z}/p^2\mathbb{Z}$ is a finer approx.



3) Repeat

- This lecture will give the shape of some proofs, but will be replete with black boxes

- Open them if and when you want to. What you find may help you in the future!

5.2 p-adic Modular Forms

- Let $A_{(p)} := \{\frac{a}{b} \in \mathbb{Q} : p \nmid b\}$ (note: usually denoted $\mathbb{Z}_{(p)}$) so $A_{(p)} = \mathbb{Z}_p \cap \mathbb{Q} \hookrightarrow$ have reduction maps $A_{(p)} \to \mathbb{Z}/p^m\mathbb{Z}$
- For $f \in M(A_{(p)})$ we often write $\overline{f} \in \mathbb{Z}/p^m\mathbb{Z}[[q]]$ for the reduction (of the coeffs) mod p^m.
- We say (f_i) is a Cauchy sequence of $f_i \in M_{k_i}(\mathbb{Q})$ if $\forall m \; \exists N : f_i, f_j \in M(A_{(p)})$ and $f_i \equiv f_j \pmod{p^m} \; \forall i, j > N$.

Definition

A <u>p-adic modular form</u> is a power series $f \in \mathbb{Q}_p[[q]]$

such that $f = \lim_i f_i$ for a sequence $(f_i) : f_i \in M(\mathbb{Q})$.

Example: p-adic Eisenstein series

- For $k \in \mathbb{N}$, let
$$\sigma_k^*(n) := \sum_{\substack{d \mid n \\ p \nmid d}} d^k.$$
Since $d \in (\mathbb{Z}/p^m\mathbb{Z})^\times$ and $|(\mathbb{Z}/p^m\mathbb{Z})^\times| = p^{m-1}(p-1)$, if $k \equiv k' \bmod p^{m-1}(p-1)$ then $\sigma_k^*(n) \equiv \sigma_{k'}^*(n) \pmod{p^m}$

- So if $k_1, k_2, k_3, \ldots$ is a sequence which is eventually stable in $\mathbb{Z}/p^{m-1}(p-1)\mathbb{Z}$ for all m, then $\sigma_{k_i}(n)$ is cauchy.

- Define $\sigma_k(n) := \lim \sigma_{k_i}^*(n)$. Then
$$G_k^* := \left(\lim_{i \to \infty} \frac{-B_{k_i}}{2k_i}\right) + \sum_{n \geq 1} \sigma_{k-1}^+(n) q^n$$
is a p-adic modular form!

Congruences of modular forms

- Return to
  - $M_k(A_{(p)}) = M_k \cap A_{(p)}[\![q]\!]$ ← wt k, coeffs in $A_{(p)}$
  - For $f = \sum a_i q^i \in M_k(A_{(p)})$, $\bar{f} := \sum \bar{a}_i q^i \in \mathbb{F}[\![q]\!]$

- $M_k(\mathbb{F}_p) = \{\bar{f} : f \in M_k(A_{(p)})\}$

- What does $M_k(\mathbb{F}_p)$ look like?

- Recall: $E_k = 1 - \frac{2k}{B_k} \sum_{n \geq 1} \sigma_{k-1}(n) q^n \in M_k(\mathbb{Q})$

  Clausen–Von Staudt theorem:

  $$p-1 \mid k \Rightarrow v_p(k/B_k) \geq 1$$

- So nonconstant terms of E_{p-1} are divisible by p, so

  $$E_{p-1} \equiv 1 \pmod{p}.$$

- For any modular form f of weight k, fE_{p-1} has weight $k+p-1$, so $\bar{f} = \overline{fE_{p-1}} \in M_{k+p-1}(\mathbb{F}_p)$

  $$M_k(\mathbb{F}_p) \subseteq M_{k+p-1}(\mathbb{F}_p) \subseteq M_{k+2(p-1)}(\mathbb{F}_p) \subseteq \cdots$$

- For $\alpha \in \mathbb{Z}/(p-1)\mathbb{Z}$, set

  $$M^{\alpha}(\mathbb{F}_p) := \bigcup_{k \equiv \alpha \pmod{p-1}} M_k(\mathbb{F}_p)$$

  closed under addition etc by preceding remark

- Further structure: $E_{p-1} - 1 \in \ker(M(A_{(p)}) \to M(\mathbb{F}_p))$, $M(A_{(p)})$ is gen. by E_4, E_6.

Theorem (Swinnerton-Dyer)

For $p \geq 5$, $M(\mathbb{F}_p) = \mathbb{F}_p(\bar{E}_4, \bar{E}_6)/(\bar{E}_{p-1} - 1)$ and

$$M(\mathbb{F}_p) = \bigoplus_{\alpha \in \mathbb{Z}/(p-1)\mathbb{Z}} M^{\alpha}(\mathbb{F}_p)$$

Proof:

Theorem: Weight congruences for congruent forms

Let $f \in M_k(A_{(p)})$, $f' \in M_{k'}(A_{(p)})$. If

$$f \equiv f' \pmod{p^m}$$

then

$$k \equiv k' \pmod{p^{m-1}(p-1)} \quad \text{if } p \geq 3$$

$$k \equiv k' \pmod{2^{m-2}} \quad \text{if } p = 2$$

If $p \geq 5$ and $m = 1$, the theorem states

$$\bar{f} = \bar{f}' \pmod{p} \Rightarrow k \equiv k' \pmod{p-1}$$

which follows from the previous theorem of Swinnerton-Dyer. $m > 1$: 

Weights of p-adic modular forms

- Let (f_i) be a Cauchy sequence of $f_i \in M_{k_i}(\mathbb{Q})$.

- So by prev. thm, $\forall m$, (k_i) stabilizes to an element K_m in $\mathbb{Z}/p^m(p-1)\mathbb{Z}$

- So we can define the weight of f as

$$k = (K_m) \in \varprojlim_m \mathbb{Z}/p^m(p-1)\mathbb{Z}$$

and note that

$$\varprojlim_m \mathbb{Z}/p^m(p-1)\mathbb{Z} \cong \varprojlim_m \left(\mathbb{Z}/p^m\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \right)$$

$$\cong \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}.$$

- So the weight of a p-adic modular form lies in $\mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$
Why is this reasonable? (Complex case)

  - Weights in $M(\Gamma)$: $f(\gamma\tau) = (c\tau+d)^k f(\tau)$
    "weights are exponents"

  - We expand this to k which can occur as an exponent of elts of $\mathbb{Z}_p^\times$"
    Problem set: n^x for $x \in \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$ makes sense/is natural

- Like for usual modular forms, nonconstant coeffs tell us about the constant coeff

Proposition
Let $f = \sum a_n q^n \in M_k(\mathbb{Q}_p)$, $k \in \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$.
If $m \geq 0$ and $k \not\equiv 0 \bmod p^n(p-1)$ then

$$v_p(a_0) + m \geq \inf_{n \geq 1} v_p(a_n)$$

Proof: If $a_0 = 0$ ✓. Else, $a_0 \in M_0(\mathbb{Q}_p)$. Since $wt(a_0) \not\equiv wt(f) \bmod p^n(p-1)$,

$$\inf_{n \geq 1}(a_n) = v_p(f - a_0) < v_p(f) + m + 1$$

↑ wt cong. thm

so $v_0(a_0) + m \geq v_p(f) + m \geq \inf_{n \geq 1} v_p(a_n)$ ●

5.3 Another Inverse Limit: $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$

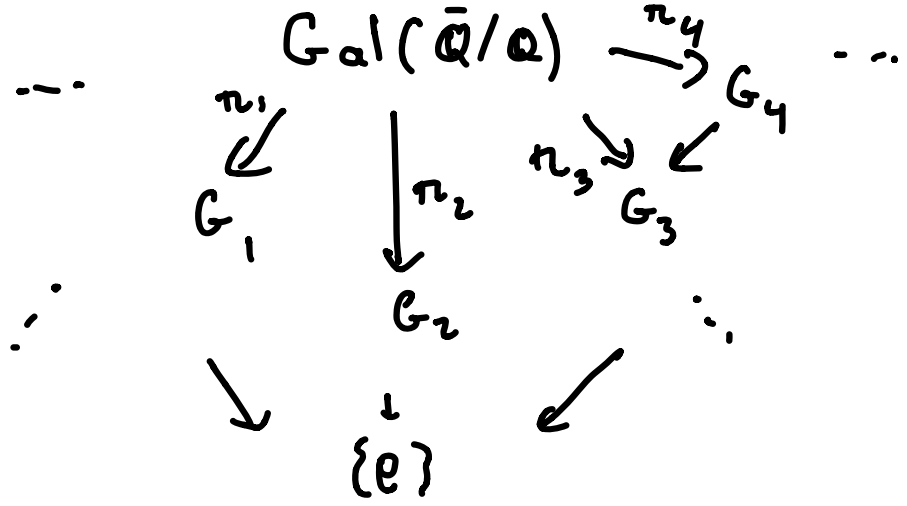
- Let $\bar{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. Then every element $\alpha \in \bar{\mathbb{Q}}$ lies in some finite Galois extension of $\mathbb{Q}$ (the splitting field of α)

- If $L/\mathbb{Q}$ is a finite Galois extension, then any automorphism $\sigma: \bar{\mathbb{Q}} \to \bar{\mathbb{Q}}$ which acts as the identity on $\mathbb{Q}$ <u>restricts to an automorphism</u> $\bar{\sigma}: L \to L$ over $\mathbb{Q}$. So we get a map

$$\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(L/\mathbb{Q})$$

which is surjective (by Zorn's Lemma)

- We want to study $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Let $\{L_i\}_{i\in I}$ be the finite Galois extensions of $\mathbb{Q}$, and let $G_i = \mathrm{Gal}(L_i/\mathbb{Q})$



- If $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ and $\alpha \in \bar{\mathbb{Q}}$, then $\alpha \in L_i$ for some $L_i/\mathbb{Q}$ finite, and $\sigma(\alpha) = (\pi_i \sigma)(\alpha)$, so

  <u>σ is determined by its images in G_i</u>

Hence $$\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \cong \varprojlim_{L/\mathbb{Q} \text{ fin. Galois}} \mathrm{Gal}(L/\mathbb{Q})$$

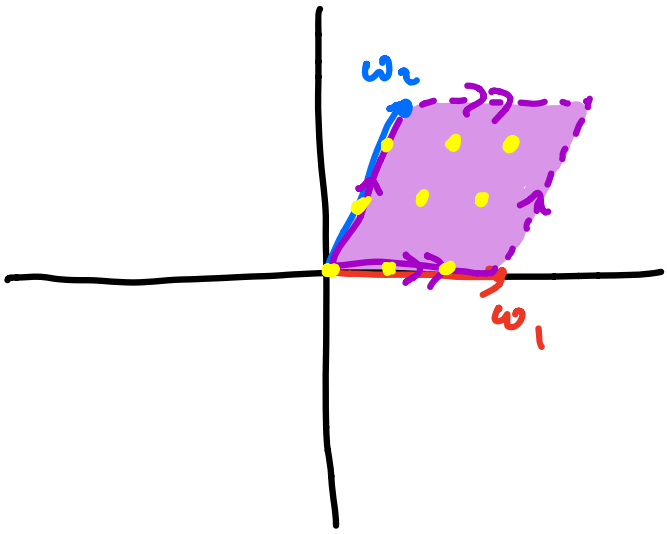
We also endow the absolute Galois group with the Krull topology, the coarsest topology such that the projections to finite quotients (with the discrete topology) are continuous.

5.4 Galois Representations

Elliptic Curve Galois Representation

- Let $E/\mathbb{Q}$ be an elliptic curve. Lets think of E as $\mathbb{C}/\Lambda$ for a lattice Λ.

Recall $E[p^n] := \{ R \in E(\mathbb{C}) : \overbrace{R + R + \cdots + R}^{p^n \text{ times}} = O \}$



3-torsion points:
$\cong (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$.

$E[p^n] \cong (\mathbb{Z}/p^n\mathbb{Z})^2$, and $E[p^n] \subseteq E(\bar{\mathbb{Q}})$.

- So $G_{\mathbb{Q}} \curvearrowright E[p^n]$, compatibly with $\cdot p$ on E, so $G_{\mathbb{Q}} \curvearrowright \varprojlim_{n\to\infty} E[p^n] \cong \varprojlim_{n\to\infty} (\mathbb{Z}/p^n\mathbb{Z})^2 \cong \mathbb{Z}_p^{\,2}$

- So $\sigma \in G_{\mathbb{Q}} \rightsquigarrow \phi_\sigma : \mathbb{Z}_p^{\,2} \to \mathbb{Z}_p^{\,2}$ automorphism
  $\wr$
  matrix in $GL_2(\mathbb{Z}_p)$

- So we get a homomorphism

$$\rho_E : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{Z}_p)$$

More generally

- Let A be a topological ring (like $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}_p$, $\mathbb{Z}_p$)

Definition
A two-dimensional Galois representation over A is a continuous homomorphism

$$\rho: G_{\mathbb{Q}} \longrightarrow GL_2(A)$$

- We can do matrix things with the matrices

$$G_{\mathbb{Q}} \xrightarrow{\rho} GL_2(A) \xrightarrow{\det} A^\times$$
$$\det \rho$$

Local Galois Groups

- Let l be a prime and let

$$G_l := Gal(\bar{\mathbb{Q}}_l / \mathbb{Q}_l)$$

$$G_\infty := Gal(\mathbb{C}/\mathbb{R})$$

- Also,

$$\begin{array}{ccc} \mathbb{Q}_l & \subset & \bar{\mathbb{Q}}_l \\ \cup & & \cup \text{ dense} \\ \mathbb{Q} & \subset & \bar{\mathbb{Q}} \end{array} \quad \circlearrowright \sigma$$

(warning: we're choosing embedding)

$\sigma|_{\bar{\mathbb{Q}}}$

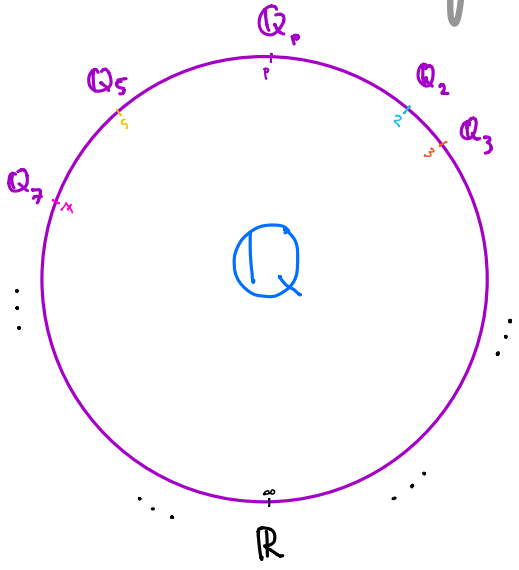
Restriction of $\sigma \in G_{\mathbb{Q}_\ell}$ to $\bar{\mathbb{Q}}$ gives a homom

$$G_\ell \to G_{\mathbb{Q}}$$

but since $\bar{\mathbb{Q}}$ is dense in $\bar{\mathbb{Q}}_\ell$, $\sigma_1|_{\bar{\mathbb{Q}}} = \sigma_2|_{\bar{\mathbb{Q}}}$ iff $\sigma_1 = \sigma_2$, so

$$G_\ell \subseteq G_{\mathbb{Q}}$$

"Automorphisms of $\bar{\mathbb{Q}}$ sending the point ℓ to the point ℓ", "Decomposition groups"



Inertia & Ramification

- We can define a subgroup of G_ℓ of automorphisms with specified behavior at the point ℓ.
- For $\ell \neq \infty$, let

$$\bar{\mathbb{Z}}_\ell := \{x \in \bar{\mathbb{Q}}_\ell \mid |x|_\ell \leq 1\} \text{ and}$$

$$\lambda := \{x \in \bar{\mathbb{Q}}_\ell \mid |x|_\ell < 1\}.$$

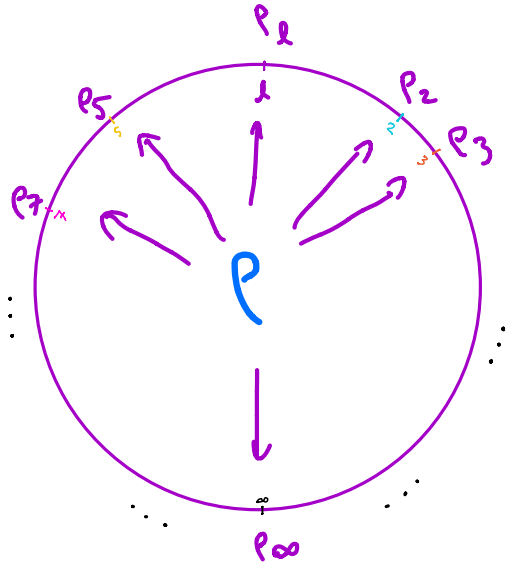
Then $\bar{\mathbb{Z}}_\ell / \lambda \cong \bar{\mathbb{F}}_\ell$ and $G_\ell \curvearrowright \bar{\mathbb{F}}_\ell$.

Definition: the inertia group

$$I_\ell := \{\sigma \in G_\ell \mid \sigma \text{ acts as id on } \overline{\mathbb{F}}_\ell\}$$

- Local properties of Galois reps
  - For a ring A and a "global" Gal. rep $\rho: G_{\mathbb{Q}} \to GL_2 A$, restrictions give local Gal reps

$$\rho|_{G_\ell}: G_\ell \longrightarrow GL_2(A)$$



Definitions: properties of a representation $\rho: G_{\mathbb{Q}} \to GL_2(A)$

- ρ is <u>odd</u> if, for c the elt of $Gal(\mathbb{C}/\mathbb{R})$ corresponding to complex conjugation, $\det \rho(c) = -1$.

- for a prime ℓ, ρ is <u>unramified at ℓ</u> if $I_\ell \subseteq \ker \rho|_{G_\ell}$

- ρ is <u>flat</u> at a prime p if $\forall$ ideals $J \subseteq A$: A/J is finite, then $\bar{\rho}: G_{\mathbb{Q}_p} \to GL_2(A/J)$ extends

to a finite flat group scheme

- ρ is <u>irreducible</u> if it has no nontrivial subrepresentation

5.5 Fermat's Last Theorem

Theorem
The equation $a^n + b^n = c^n$ has no nontrivial integer solns ($abc \neq 0$) if $n \geq 3$

Proof (lol)

$(a^m)^p + (b^m)^p = (c^m)^p \rightsquigarrow$ reduce to prime exponent.

- Suppose for contradiction that $a^p + b^p = c^p$, a, b, c coprime

- Frey curve

$$E_{a^p, b^p, c^p} : y^2 = x(x - a^p)(x + b^p)$$

- The Galois representation associated to this curve has some remarkable properties:

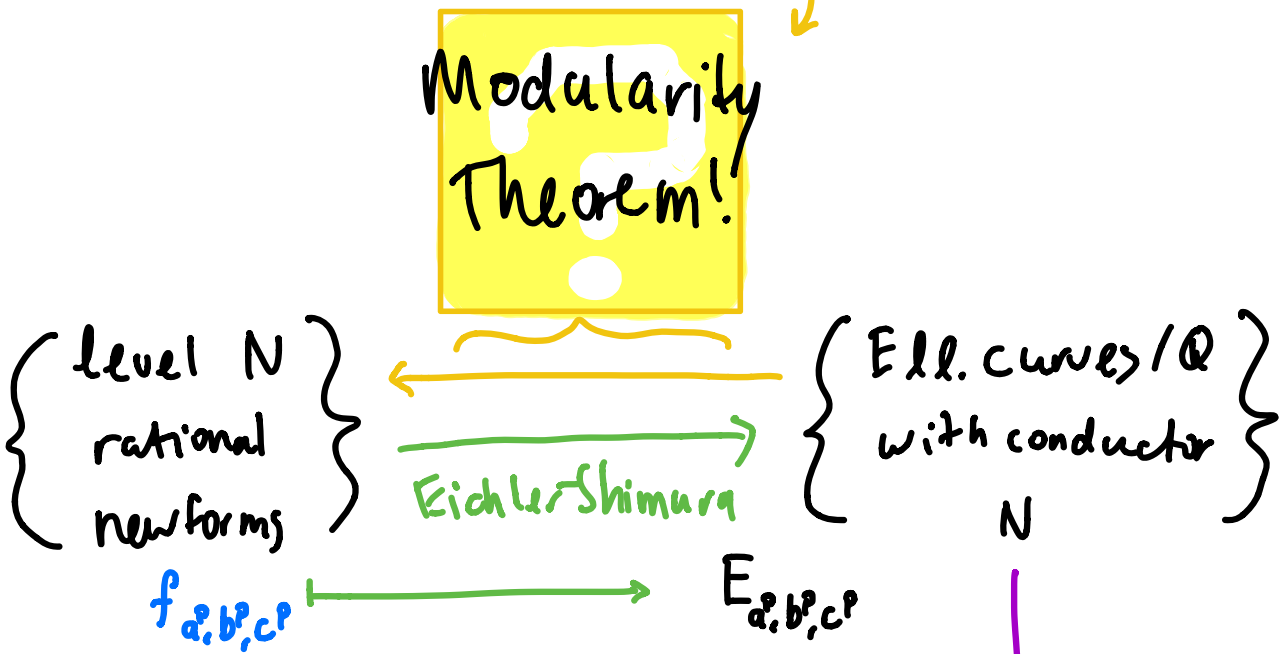
Theorem: Frey, Serre
Let $p \geq 5$ prime and $a, b, c \in \mathbb{Z}$: $a^p + b^p + c^p = 0$ $abc \neq 0$

Suppose $a \equiv -1 \pmod 4$ and $2 \mid b$. Then $\bar{\rho}_{a^p,b^p,c^p}$ is absolutely irreducible, odd, and unramified outside of $2, p$ and flat at p.

- In fact, people suspect that no Galois rep. has these properties.
- We try to get at $\bar{\rho}_{a^p,b^p,c^p}$ another way, via modular forms
- Eichler–Shimura construction: way of associating elliptic curve to "level N rational newform"

$f \longrightarrow E_f$ s.t.
- Conductor N of E_f = level of f
- $a_p(E)$ encode coeffs of f

Wiles, Taylor–Wiles, Breuil–Conrad–Diamond–Taylor



$g \in S_2(\Gamma_0(2))$:

ρ_{a^p,b^p,c^p}

$\{$ Galois Representations $\rho: G_{\mathbb{Q}} \to GL_2(\mathbb{Z}_p)\}$

Theorem: Ribet

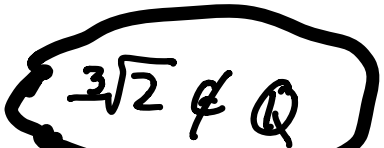
Let f be a weight 2 newform of level N, and let l be a prime s.t. $l \mid N$ but $l^2 \nmid N$. Suppose $\bar{\rho}_f$ is absolutely irreducible and and that one of the following is true:

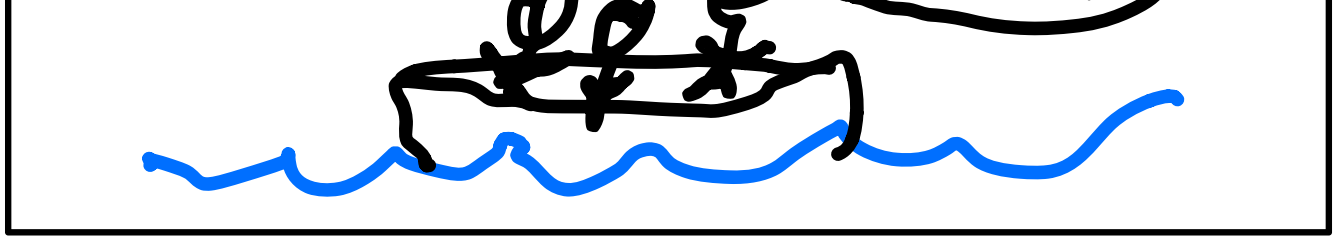
- $\bar{\rho}_f$ is unramified at l or
- $l = p$ and $\bar{\rho}_f$ is flat at p

Then there is a weight 2 newform g of level N/l s.t. $\bar{\rho}_f \cong \bar{\rho}_g$

Proof of FLT: E_{a^p,b^p,c^p} has an associated modular form f_{a^p,b^p,c^p} by Modularity Theorem. And $\bar{\rho}_{a^p,b^p,c^p}$ is "barely ramified" etc by Frey-Serre. So can apply Ribet's Theorem iteratively to the primes dividing the conductor $N = \prod_{l \mid abc} l$ since N is square free; this procedure produces a newform g of wt 2 and level 2. But the space of lvl 2 wt 2 cusp forms $S_2(\Gamma_0(2))$, has dim = genus$(X_0(2)) = 0$ (Dr. Watsons lectures). So there is no such form g, a contradiction!

Corollary





Proof: Let $c := \sqrt[3]{2}$. If c were in $\mathbb{Q}$,

$$1^3 + 1^3 = c^3$$

would be a rational solution to $a^3 + b^3 = c^3$. But there is no such solution by FLT ∎

The real reason we care about FLT is the friends we made along the way!