5.1 Inverse Limit Mathematics

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

- Lec i n'est pas Zp

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 approach.

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 \( \mathbb{Z}_p^\times \)) so \( A_p = \mathbb{Z}_p \cap \mathbb{Q} \) have reduction maps \( A_p \to \mathbb{Z}/p^\infty \mathbb{Z} \).

- For \( f \in M(A_p) \) we often write \( \overline{f} \in \mathbb{Z}/p^\infty \mathbb{Z}[[q]] \) for the reduction (of the coeff) \( \mod p^m \).

- We say \( (f_n) \) is a Cauchy sequence of \( f_n \in M_k(\mathbb{Q}) \) if 
  \[ \forall m \in \mathbb{N} : f_n, f_j \in M(A_p) \text{ and } f_n \equiv f_j \pmod{p^m} \forall n, j \geq N. \]

**Definition**

A \( p \)-adic modular form is a power series \( f \in \mathbb{Q}_p[[q]] \).
such that \( f = \lim f_i \) for a sequence \((f_i) : f_i \in M(Q)\).

**Example: \( p \)-adic Eisenstein series**

- For \( k \in \mathbb{N} \), let
  \[
  \sigma_k^*(n) := \sum_{d \mid n, \text{pd}} d^k.
  \]

  Since \( d \in (\mathbb{Z}/p^m \mathbb{Z})^* \) and \( l(\mathbb{Z}/p^m \mathbb{Z}) l = p^{m-1}(p-1) \),
  if \( k \equiv k' \mod p^{m-1}(p-1) \) then \( \sigma_k^*(n) \equiv \sigma_{k'}^*(n) \mod p^m \).

- 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 \( \sigma_k^*(n) \) is Cauchy.

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

**Congruences of modular forms**

- Return to
  - \( M_k(A_{(p)}) = M_k \cap A_{(p)} \bigcup q \bigcup \) \( \left< \omega^+ b, (\text{coeffs in } A_{c_{(p)}}) \right> \)
  - For \( f = \sum q \cdot \phi_i \in M_k(A_{(p)}) \), \( f := \sum \phi_i \cdot (\text{coeffs in } A_{(p)}) \)
What does $M_k(\mathbb{F}_p)$ look like?

Recall:

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

Clausen–Von Staudt theorem:

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

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 $f = fE_{p-1} \in M_{k+p-1}(\mathbb{F}_p)$

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

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: $E_{p-1} - 1 \in ker(M(A_0) \to M(\mathbb{F}_p))$, $M(A_0)$ is gen. by $E_4$, $E_6$. 


Theorem (Swinnerton-Dyer)

For \( p \geq 5 \), \( M(\mathbb{F}_p) = \overline{\mathbb{F}_p}(E_4, E_6)/(E_{p-1} - 1) \) and
\[
M(\mathbb{F}_p) = \bigoplus_{\alpha \in \mathbb{Z}/p-1} M^\alpha(\mathbb{F}_p)
\]

Proof:

\[ ? \]

Theorem: Weight congruences for congruent forms

Let \( f \in M_k(A_{\mathbb{F}_p}) \), \( f' \in M_{k'}(A_{\mathbb{F}_p}) \). 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
\[
f \equiv f' \pmod{p} \Rightarrow k \equiv k' \pmod{p-1}
\]
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, \(V_{M_i}(k_i)\) stabilizes to an element \(K_m\) in \(\mathbb{Z}/p^m(p-1)\mathbb{Z}\).

So we can define the weight of \(f\) as

\[ k = (K_m) \in \lim_{\to m} \mathbb{Z}/p^m(p-1)\mathbb{Z} \]

and note that

\[ \lim_{\to m} \mathbb{Z}/p^m(p-1)\mathbb{Z} \cong \lim_{\to m} \left( \mathbb{Z}/p^m \mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \right) \]

\[ = \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z} \]

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 cans)

- Weights in \(M(C)\): \(f(\mathfrak{a}z) = (cz + d)^k f(z)\)
  "weights are exponents"

- We expand this to \(k\) which can occur as an exponent of \(\mathfrak{a}\) of \(\mathbb{Z}_p^x\)

Problem set: \(n^k\) 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 \( f = \sum a_n q^n \in M_{m, \infty}(\mathbb{Q}_p) \), \( k \in \mathbb{Z}_p \times \mathbb{Z}/(\mathbb{Z}_p \setminus \{0\}) \).
If \( m \geq 0 \) and \( k \neq 0 \mod p^n(p-1) \) then
\[
V_p(a_0) + m \geq \inf_{n \in \mathbb{Z}_\mathbb{N}} V_p(a_n)
\]

Proof: If \( a_0 = 0 \) \( \forall \). Else, \( a_0 \in M_{m, \infty}(\mathbb{Q}_p) \). Since
\[
wt(a_0) \neq wt(f) \mod p^n(p-1),
\]
\[
\inf(a_0) = V_p(f-a_0) < V_p(f) + m + 1
\]
so
\[
V_0(a_0) + m \geq V_p(f) + m \geq \inf_{n \in \mathbb{Z}_\mathbb{N}} V_p(a_n)
\]

5.3 Another Inverse Limit: \( \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \)

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

- If \( L/\mathbb{Q} \) is a finite Galois extension, then
  any automorphism \( \sigma: \overline{\mathbb{Q}} \rightarrow \overline{\mathbb{Q}} \) which acts
  as the identity on \( \mathbb{Q} \) restricts to an automorphism
  \( \sigma: L \rightarrow L \) over \( \mathbb{Q} \). So we get a map

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

If $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and $\alpha \in \overline{\mathbb{Q}}$, then $\alpha \in L_i$ for some $L_i/\mathbb{Q}$ finite, and $\sigma(\alpha) = (\pi_i \circ \sigma)(\alpha)$, so $\sigma$ is determined by its images in $G_i$.

Hence $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \varprojlim_{i \in I} \text{Gal}(L_i/\mathbb{Q})$.

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. Let's think of $E$ as $\mathbb{C}/\Lambda$ for a lattice $\Lambda$. 
Recall $E[p^n] := \{ R \in E(C) : R + R + \cdots + R = O \}$.

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

. So $G_{\overline{\mathbb{Q}}} \cong E[p^n]$, compatibly with $p$ on $E$, so

$$G_{\overline{\mathbb{Q}}} \cong \varinjlim_{n \to \infty} E[p^n] \cong \varinjlim_{n \to \infty} (\mathbb{Z}/p^n\mathbb{Z})^2 \cong \mathbb{Z}_p^2$$

. So $\sigma \in G_{\overline{\mathbb{Q}}} \Rightarrow \phi : \mathbb{Z}_p^2 \to \mathbb{Z}_p^2$ automorphism matrix in $GL_2(\mathbb{Z}_p)$

. So we get a homomorphism

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

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

**Definition**

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

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

- We can do matrix things with the matrices

$$G_\mathbb{Q} \xrightarrow{\rho} GL_2(A) \xrightarrow{\text{det}^+} A^x$$

Local Galois Groups

- Let $l$ be a prime and let
  $$G_l := \text{Gal}(\overline{\mathbb{Q}_l}/\mathbb{Q}_l)$$
  $$G_\infty := \text{Gal}(\mathbb{C}/\mathbb{R})$$

- Also,
  $$\mathbb{Q}_l \subset \overline{\mathbb{Q}}_l$$
  $$\mathbb{U} \subset U_{\text{dense}}$$
  $$\mathbb{Q} \subset \overline{\mathbb{Q}}$$

(warning: we're choosing embedding)
Restriction of $\sigma \in G_{\overline{\mathbb{Q}}_l}$ to $\overline{\mathbb{Q}}$ gives a homomorphism $G_{\mathbb{Q}} \to G_{\overline{\mathbb{Q}}}$, but since $\overline{\mathbb{Q}}$ is dense in $\overline{\mathbb{Q}}_l$, $\sigma, 1 \overline{\mathbb{Q}} = \sigma_2 \overline{\mathbb{Q}}$ iff $\sigma_1 = \sigma_2$, so $G_{\mathbb{Q}} \subseteq G_{\overline{\mathbb{Q}}}$.

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

**Inertia and Ramification**

- We can define a subgroup of $G_l$ of automorphisms with specified behavior at the point $l$.
- For $l \neq \infty$, let
  
  $$\Xi_l := \{ x \in \overline{\mathbb{Q}}_l | |x|_l \leq 1^3 \}$$

  and

  $$\lambda := \{ x \in \overline{\mathbb{Q}}_l | |x|_l < 1^3 \}.$$

Then $\Xi_l \lambda = \Xi_l$ and $G_l \supseteq \Xi_l$.
Definition: the inertia group
\[ I_e := \{ \sigma \in G_F \mid \sigma acts as id on \overline{F}_F \} \]

- Local properties of Galois reps
  - For a ring \( A \) and a "global" Gal. rep \( \rho : G_\mathbb{A} \to GL_2 A \), restrictions give local Gal reps
  \[ \rho|_{G_F} : G_F \to GL_2(A) \]

Definitions: properties of a representation \( \rho : G_\mathbb{A} \to GL_2(A) \)
- \( \rho \) is odd if, for \( c \) the elt of Gal(\( \mathbb{C}/\mathbb{R} \)) corresponding to complex conjugation, \( \det \rho(c) = -1 \).
- For a prime \( l \), \( \rho \) is unramified at \( l \) if \( I_e \subseteq \ker \rho|_{G_l} \).
- \( \rho \) is flat at a prime \( p \) if \( \forall \) ideals \( J \subseteq A : \nabla(J) \) is finite, then \( \tilde{\rho} : G_{\mathbb{Q}_p} \to GL_2(\mathbb{A} / \mathbb{F}_p) \) extends.
In a finite flat group scheme
- $\Phi$ is irreducible if it has no nontrivial subrepresentation.

5.5 Fermat's Last Theorem

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

**Proof ( heed )**

$(a^n)p + (b^n)p = (c^n)p \rightarrow$ reduce to prime exponent.
- Suppose for contradiction that $a^n + b^n = c^n$, $a,b,c$ coprime

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

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

**Theorem: Frey Curve**
Let $p \geq 5$ prime and $a,b,c \in \mathbb{Z} : a^p + b^p + c^p = 0 \implies 0$. 

---

Theorem: Frey, Sure
Suppose \( a \equiv -1 \pmod{4} \) and \( 2 \mid b \). Then \( \overline{E}_{a,b,c} \) 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 \( \overline{E}_{a,b,c} \) another way, via modular forms.

- Eichler–Shimura construction: way of associating elliptic curve to "level N rational newform"

\[
\begin{align*}
  f & \mapsto E_f \\
  & \text{s.t.} \quad \text{Conductor } N \text{ of } E_f = \text{level of } f \\
  & \text{and } \quad a_p(E) \text{ encode } \langle \alpha_{p,E} \rangle \\
\end{align*}
\]

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

---

Modularity Theorem!

\[
\begin{align*}
\{ \text{level N rational newforms}\} & \xleftarrow{\text{Eichler–Shimura}} \{ \text{Ell. curves } \mathbb{Q}\text{ with conductor } N \} \\
\{ f_{a,b,c} \} & \xrightarrow{\text{Eichler–Shimura}} \{ E_{a,b,c} \}
\end{align*}
\]
Theorem: Ribet

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

- \( \overline{\rho}_f \) is unramified at \( l \) or
- \( l = \mathfrak{p} \) and \( \overline{\rho}_f \) is flat at \( \mathfrak{p} \)

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

Proof of FLT: \( E_{a,b,c} \) has an associated modular form \( f_{a,b,c} \) by Modularity Theorem. And \( \overline{\rho}_{a,b,c} \) is “barely ramified” etc by Frey-G lower. So can apply Ribet’s Theorem iteratively to the primes dividing the conductor \( N = \prod l \).

Since \( N \) is square-free, this procedure produces a newform \( g \) of wt 2 and level 2. But the space of wt 2 cusp forms \( S_2(\Gamma_0(2)) \) has dim \( = \dim \) gens \( (X_0(2)) = 0 \) (Dr. Watson’s lectures). So there is no such form \( g \), a contradiction!

Corollary

\( \sqrt{2} \notin \mathbb{Q} \)
Proof: Let $c := 2\sqrt{2}$. 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!