Elliptic curve, Fermat Last Thm & modularity lifting.

p, ℓ primes, $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, $\mathbb{F}_\ell := \mathbb{Z}/\ell\mathbb{Z}$.

I proof of FLT via modularity lifting

FLT $\quad a^n + b^n \neq c^n, \quad \forall\, a, b, c \in \mathbb{N}, \quad n \geq 3.$

Thm (Taniyama - shimura - wiles +) Any elliptic curve (EC) $/\mathbb{Q}$ is modular.

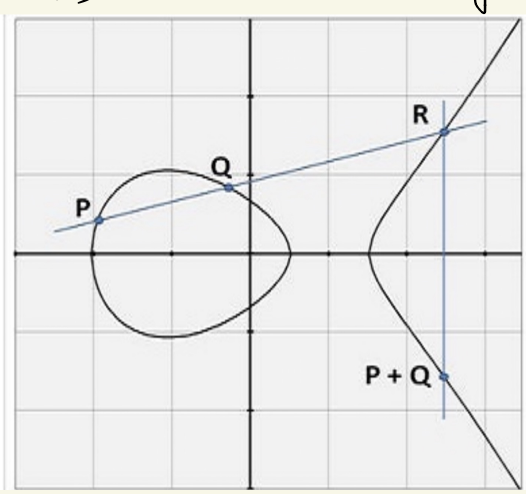
If $a, b, c \in \mathbb{N}$ satisfies $a^\ell + b^\ell = c^\ell$, $\ell \geq 3$, then Frey curve
$E: \; y^2 = x(x - a^\ell)(x + b^\ell)$ is NOT moduler. contradiction!
$\therefore$ FLT holds.

II Elliptic Curve:

Def: An EC $/\mathbb{Q}$ is a projective curve given by Weierstrass Eqn

$$E: \; y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Q}$$
$$\Delta = 4a^3 + 27b^2 \neq 0.$$

Fact: ① $E(K)$ is an abelian group for $K/\mathbb{Q}$ a field ext.



② $E(\mathbb{C}) \simeq$  $\simeq S \times S$ where $S = \mathbb{C}/\mathbb{Z}$.

Set $E[p^n] := \{ x \in E(\mathbb{C}) \mid p^n x = \underbrace{x + \cdots + x}_{p^n} = 0 \}$

Then $E[p^n] \simeq \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z}$

Note $G_{\mathbb{Q}} \curvearrowright E[p^n]$ as E is defined $/\mathbb{Q}$.

Def : The p-adic Tate module $T_p(E) := \varprojlim_n E[p^n] \simeq \mathbb{Z}_p \times \mathbb{Z}_p$

Note $G_{\mathbb{Q}} \curvearrowright T_p(E)$ continuously $\rightsquigarrow$ $\rho_E : G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{Z}_p} T_p(E) = GL_2(\mathbb{Z}_p)$.

III p-adic Galois representation

Let $K/\mathbb{Q}_p$ be a p-adic field with residue field $k/\mathbb{F}_p$.

Def : A p-adic Galois rep. is a pair (ρ, V) where

① V is a finite dim. K-V.S.

② $\rho : G_{\mathbb{Q}} \longrightarrow GL(V)$ is a continuous group homo.

Example ① cyclotomic character $\chi_p : G_{\mathbb{Q}} \to \mathbb{Z}_p^\times \le GL_1(\mathbb{Q}_p)$ defined by $g(\zeta_{p^n}) = \zeta_{p^n}^{\chi_p(g) \bmod p^n}$ where ζ_{p^n} primitive p^n-th root of unity.

② $V_p(E) := T_p(E)[\frac{1}{p}]$.

Fact : Given a p-adic rep. (ρ, V), $\exists$ a $\mathcal{O}_K$-lattice $T \subseteq V$ so that $g(T) \subseteq T$, $\forall g \in G_{\mathbb{Q}}$. So

$$\begin{tikzcd} G_{\mathbb{Q}} \arrow[r, "\rho"] \arrow[dr, "\rho_n"'] & \mathrm{Aut}_{\mathbb{Z}_p}(T) \simeq GL_d(\mathcal{O}_K) \arrow[d, "\bmod \pi^n"] \\ & GL_d(\mathcal{O}_K/\pi^n) \end{tikzcd}$$

π uniformizer of $\mathcal{O}_K$

Def : $\bar\rho = \rho_1 = \rho \bmod \pi : G_{\mathbb{Q}} \longrightarrow GL_d(k)$ is called the reduction of ρ.

Remark : $\bar\rho$ may depend on the choice of T. But its semi-simplification $\bar\rho^{ss}$ is independent of T.

IV Local properties of (ρ, V)

$\forall\, \ell$ prime. Let G_ℓ be decomposition subgp of $G_{\mathbb{Q}}$ at ℓ.

Then $G_\ell \simeq \mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$. To explain this, recall $G_{\mathbb{Q}} = \varprojlim_{F \text{ finite Galois}} \mathrm{Gal}(F/\mathbb{Q})$

$$\begin{array}{cc} F & \ell_1 \cdots \ell_m \\ | & | \\ \mathbb{Q} & \ell \end{array} \qquad \begin{aligned} G_{\ell_1} &= \{\sigma \in \mathrm{Gal}(F/\mathbb{Q}) \mid \sigma(\ell_1) = \ell_1\} \\ &\simeq \mathrm{Gal}(F_{\ell_1}/\mathbb{Q}_\ell). \end{aligned}$$

Recall

$$0 \to I_\ell \to G_\ell \to \mathrm{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}_\ell) \to 0$$

Inertia gp at ℓ. $\quad \mathrm{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}_\ell) = \widehat{\langle \mathrm{Fr}_\ell \rangle}$ where $\mathrm{Fr}_\ell(x) = x^\ell$, $\forall x \in \overline{\mathbb{F}}_\ell$, called <u>Frobenius at ℓ</u>

<u>Def</u>: ρ is called <u>unramified at ℓ</u> if $\rho(I_\ell) = I_d$ = idenity matrix.

$\iff \rho(\mathrm{Fr}_\ell)$ makes sense.

<u>Example</u>: ① χ_p is unranfied $\forall\, \ell \neq p$, $\chi_p(\mathrm{Fr}_\ell) = \ell$.

② (Néron - Ogg - Shafarevich) $\forall\, \ell \neq p$, E has good reduction $/\ell$

$\iff T_p(E)$ is unramified at ℓ.

Here E has good reduction $/\ell \iff E \bmod \ell$ is still an E.C.

e.g. when $\ell \nmid \Delta$.

V Modular form:

Let $N \geq 1$, $\mathcal{H} \leq \mathbb{C}$ upper half plane.

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

<u>Def</u>: A <u>modular form</u> of weight $k \geq 2$ & level N is a holomorphic function $f: \mathcal{H} \to \mathbb{C}$ so that

① $f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z) \quad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N)$.

② $f(z)$ is "good" at cusps.

$\Downarrow$

$$f(z) = \sum_{n=1}^{\infty} a_n(f)\, q^n \quad \text{with } q = e^{2\pi i z}$$

Let $S_k(\Gamma_1(N)) = \{$ modular form of weight k, level $N \}$.

Conjecture (Taniyama - Shimura) Given an elliptic curve $E/\mathbb{Q}$, E is modular

i.e., $\exists\, f \in S_2(\Gamma_1(N))$ so that for $\ell >> 0$

$$a_\ell(f) = \mathrm{trace}\,(\rho_E(\mathrm{Fr}_\ell)).$$

Remark: E is modular $\Leftrightarrow$ $\exists$ morphism $\mathcal{H}/\Gamma_1(N) \twoheadrightarrow E$.

If Frey Curve is moduler $\Rightarrow$ $N=2$ when $a^n+b^n=c^n$.

But $\mathcal{H}/\Gamma_1(2)$ has genus 0 while E has genus 1, contradiction!

Conjecture (Fontaine - Mazur)

Let F be a # field, $\rho: G_F \to GL(V)$ a p-adic rep.

Assume ① ρ is unramfied for almost all prime $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_F)$

② For prime $\mathfrak{p} \mid p$, $\rho|_{G_\mathfrak{p}}$ is de Rham.

Then ρ comes from an automorphic form of $GL_n(\mathbb{A}_F)$.

VI Wiles' strategy on modularity lifting.

1 Serre's conjecture

Suppose $\bar{\rho}: G_\mathbb{Q} \to GL_2(\overline{\mathbb{F}}_p)$ is irreducible rep. Then $\exists$ moduler form $f \in S_k(\Gamma_1(N))$ so that

$$a_\ell(f) \bmod p = \mathrm{trace}\,(\bar{\rho}(\mathrm{Fr}_\ell)) \quad \text{for } \ell >> 0$$

Remark: ① The precise version, which predict "minimal" k, N implies that $E/\mathbb{Q}$ is moduler.

② Now Serre's conj is a theorem by Khare – Wintenberger

③ For Wiles, he only knew Serre's conj for $p = 2, 3$ & certain cases of $p = 5$.

2 Galois deformation:

Fix a residue rep: $\bar\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{F})$, $\mathbb{F}/\mathbb{F}_p$ finite.

$\tilde\rho : G_{\mathbb{Q}} \to GL_2(\mathcal{O}_K)$ is called a deformation of $\bar\rho$ if $\tilde\rho \bmod \pi \simeq \bar\rho$. Then there exists a universal deformation ring $R_{\bar\rho}$, and $\rho^{univ} : G_{\mathbb{Q}} \to GL_2(R_{\bar\rho})$ which "parametrize" all deformation of $\bar\rho$.

It is known that all "modular deformation" live in the family $\rho^{mod} : G_{\mathbb{Q}} \to GL_2(\mathbb{T}_p)$ where $\mathbb{T}$ is a certain Hecke algebra.

Now we have

$$\begin{tikzcd}
G_{\mathbb{Q}} \arrow[r] \arrow[d] & GL_2(R_{\bar\rho}) \arrow[dl] \arrow[dr, "\rho_E"] \arrow[dd] & \\
GL_2(\mathbb{T}_p) \arrow[rr, dashed, "?"] \arrow[dr, "\sim"'] & & GL_2(\mathbb{Z}_p) \\
& GL_2(R^{fl}_{\bar\rho}) \arrow[ur] &
\end{tikzcd}$$

by input of known Serre's conjecture.

we need to show blue arrow exists.

Wiles introduces the idea "flat deformation" $R^{fl}_{\bar\rho}$ and show that $R^{fl}_{\bar\rho} \simeq \mathbb{T}_p$. ($R = T$ thm) together with Taylor.

VII Structure of $G_\ell \simeq Gal(\bar{\mathbb{Q}}_\ell / \mathbb{Q}_\ell)$

Recall $0 \to I_\ell \to G_\ell \to Gal(\bar{\mathbb{F}}_\ell / \mathbb{F}_\ell) \to 0$.

$$Gal(\bar{\mathbb{F}}_\ell / \mathbb{F}_\ell) \simeq \widehat{\langle Fr_\ell \rangle} \simeq \hat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z}.$$

$0 \to I^w \to I_\ell \to I_\ell^t \to 0$

I^w is wild inertia which pro-p group. I_ℓ^t is tame inertia.

$$I_\ell^t \simeq \prod_{p \nmid \ell} \mathbb{Z}_p(1) = \mathrm{Gal}\left(\bigcup_{\ell \nmid m} \mathbb{Q}_\ell(\sqrt[m]{\ell}) / \mathbb{Q}_\ell \right)$$

Here (1) means that if $F \in I_\ell$ be a lift of Fr_ℓ. $\forall \sigma \in \mathbb{Z}_p(1)$ then $F \sigma F^{-1} = \sigma^\ell$.

We have filtration on I_ℓ to define conductor. But need sb discuss in details.

VIII Chebotarev Density

Thm: Let $F/\mathbb{Q}$ be a Galois extension which is unramified over a finite set S of primes then $\bigcup_{p \notin S} [\mathrm{Fr}_p]$ is dense in $\mathrm{Gal}(F/\mathbb{Q})$.

Here Fr_p is a conjugacy class of Frobenius at p.

Application: If an irreducible p-adic Galois rep. ρ is unramified for all most all prime ℓ. then ρ is uniquely determined by the trace $(\rho(\mathrm{Fr}_\ell))$, $\ell >> 0$.

See [PDT] prop 2.6 for more general & precise statements.

IX Review class field Theory

a) Local class field Theory:

Let K be a p-adic field. Then $\exists$ local Artin map $\theta_K : K^\times \longrightarrow G_K^{ab}$

so that ① $\theta_K(\pi) = \mathrm{Fr}_p$.

② For L/K finite abelian then θ_K induces an isomorphism

$$\theta_L : K^\times / N_{L/K}(L^\times) \xrightarrow{\sim} \mathrm{Gal}(L/K).$$

③ $\theta_K |_{O_K^\times} : O_K^\times \xrightarrow{\sim} I_p^{ab}$

Example: $\mathbb{Q}_p^{ab} \simeq \bigcup_{p \nmid m} \mathbb{Q}(\zeta_m) \cup \bigcup_{n \geq 1} \mathbb{Q}(\zeta_{p^n})$. $\theta_K : \mathbb{Z}_p^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$

which is given by $\theta_K = \chi_p^{-1}$.

b) Global class field theory:

Let F be a # field. $\mathbb{I}_F$ the idele group of F. Then $\exists$ global Artin map $\theta_F : \mathbb{I}_F \longrightarrow G_F^{ab}$ so that

i) $\theta_F|_{F_v} = \theta_{F_v}$ in LCF.

ii) $\theta_F|_{F^\times} = 1$

iii) For any finite abelian ext L/F, θ_F induces an isomorphism
$$\mathbb{I}_F / F^\times N_{L/F}(\mathbb{I}_L) \xrightarrow{\sim} \mathrm{Gal}(L/F).$$

when $F = \mathbb{Q}$, we have $G_{\mathbb{Q}}^{ab} \simeq \prod_p \mathbb{Z}_p^\times \simeq \mathrm{Gal}\left(\bigcup_n \mathbb{Q}(\zeta_n) / \mathbb{Q}\right)$.
given by $\prod_p \chi_p$.