Título:

Demostración de la Conjetura de Serre:

Ideas centrales y simplificaciones.

Resumen: En esta charla recordaremos los principales resultados de Wiles y Taylor en los que se apoya la demostración de la conjetura de modularidad de Serre y las herramientas creadas por el orador, Khare y Wintenberger que permitieron su completa demostración en el período 2004-2007.

Mencionaremos también un nuevo teorema "tipo Wiles" de Luc Pan y cómo utilizándolo se simplifica la prueba de la conjetura.

Luis Dieulefait

(Catedrático de Álgebra, Universitat de Barcelona).

Seminario Latinoamericano de Teoría de Números,

22 de Octubre de 2020.

Enunciado de la Conjetura:

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

una representación de Galois, donde $G_{\mathbb{Q}} = Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ y

k es un cuerpo finito de característica $p>2$.

Supongamos que ρ es impar: o sea: si c es la conjugación

compleja $\rho(c)$ es una matriz de orden 2 conjugada a $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Y que ρ es absolutamente irreducible.

(1987) ← Serre conjeturó que una tal ρ siempre es modular, es decir, que

existe una forma modular $f \in S_k^{new}(N)$ con $k \geq 2$ que es

forma propia para el álgebra de Hecke tal que si $\mathbb{Q}_f$ es

el cuerpo de coeficientes de f, es decir, el cuerpo de números

generado por los autovalores a_p de f: $\mathbb{Q}_f = \mathbb{Q}(\{a_p\})$

(f se supone normalizada: es decir $a_1(f) = 1$) y un primo

β de $\mathbb{Q}_f$ dividiendo a p tal que si consideramos la representación

de Galois β-ádica continua: (construida por Eichler-Shimura y

Deligne): $\rho_{f,\beta}: G_{\mathbb{Q}} \to GL_2(\mathcal{O}_{\mathbb{Q}_f,\beta})$

asociada a f y su reducción módulo β, que llamaremos $\overline{\rho}_{f,\beta}$, se tiene:

$$\rho \cong \overline{\rho}_{f,\beta}.$$

Además, Serre predijo, en la versión fuerte de la conjetura, un valor para el peso de la forma modular, y el nivel, no como únicos valores posibles pero como valores "óptimos" en un cierto sentido: ambos valores se conocen como:

$k(\rho)$: peso de Serre de ρ

$N(\rho)$: nivel de Serre de ρ

y los definió en términos exclusivamente de ρ.

Veamos la definición:

$N(\rho)$: parte prima con p del conductor de ρ.

$k(\rho)$: este valor se define en término de la restricción $\rho|_{I_p}$. Como tuvistado por una apropiada potencia de χ = caracter ciclotómico módulo p podemos suponer que estamos en uno de los casos siguientes, lo definiremos por simplicidad sólo en este caso:

(1) $\rho|_{I_p} \simeq \begin{pmatrix} \chi^r & * \\ 0 & 1 \end{pmatrix}$ $\quad 1 \le r \le p-1$.

o (2) $\rho|_{I_p} \simeq \begin{pmatrix} \psi_2^a & 0 \\ 0 & \psi_2^{ap} \end{pmatrix}$ $\quad 1 \le r \le p-1$.

donde ψ_2 es un carácter fundamental de "nivel 2".

Entonces el peso de Serre se define en todos los casos como $r+1 = k(\rho)$ (luego $k(\rho)$ está entre 2 y p) excepto si se está en el caso (1) con $r=1$: en este caso $k(\rho)$ puede valer o 2 o $p+1$, y esto depende del tipo de ramificación de la entrada $(1,2)$ de la matriz $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$. Si la extensión asociada a esta entrada es "poco ramificada" entonces se tiene $k(\rho)=2$: este caso es equivalente a pedir que $\rho|_{D_p}$, donde D_p es un grupo de descomposición en p, es la representación de Galois asociada a una variedad abeliana sobre $\mathbb{Q}_p$ con buena reducción en p, o más generalmente, a un esquema en grupo finito y flat sobre $\mathbb{Q}_p$ (o a un p-divisible group, o que es Barsotti-Tate, o que es cristalino de peso 2).

En el caso complementario llamado "tres ramifica" tenemos que $k(e)=p+1$.

Este caso ocurre por ejemplo (en general) si consideramos la representación módulo p asociada a una curva elíptica sobre $\mathbb{Q}_p$ (o variedad abeliana de tipo $\mathbb{Q}_{-2}$) con reducción multiplicativa en p.

Es decir que para $p=1$ tanto si toca $k(e)=2$ o $k(e)=p+1$ la representación es del tipo que proviene de una variedad abeliana:

en el caso "buena reducción en p" ponemos $k(e)=2$ y en el caso contrario lo "lógico" sería poner también $k(e)=2$ pero por ser un caso de mala reducción en p debería ser $p \mid N(e)$. Como, por convención, Serre decidió fijar $N(e)$ coprimo con p, y ahí es explotar la congruencia que él mismo estudiaba en los '70:

$$S_2(p \cdot N') \equiv S_{p+1}(N') \quad , \quad (p \text{ coprimo con } N')$$

que es la razón que le permite coger siempre $N(e)$ coprimo con p a expensas de manipular el valor de $k(e)$.

En los años 80 la obra de varios matemáticos, principalmente resultados de Ribet (level-lowering) y Edixhoven (estudio de posibles pares), permitió probar la equivalencia:

(versión débil) Conjetura de Serre $\Leftrightarrow$ versión fuerte de Conjetura de Serre.

De todos modos, sería un error pensar que al probar la conjetura es apropiado "olvidarse de $k(\epsilon)$ y $N(\epsilon)$" pues hasta con probar la versión débil.

Por el contrario, hay que "heredar el conocimiento" generado por los pioneros para probar directamente la versión fuerte, explotando el conocimiento (y control) de los invariantes $k(\epsilon)$ y $N(\epsilon)$.

Herramientas de Wiles y Taylor:

Las 2 herramientas claves para la demostración son:

(1) Teoremas de levantamiento modular (Wiles, Taylor-Wiles, Kisin...)

(2) Teorema de modularidad potencial (Taylor).

(1) Desarrollado en el transcurso de la demostración del teorema de Fermat, esta herramienta se aplica al caso de una representación ρ-ádica:

$$\hat{\rho} : G_{\mathbb{Q}} \longrightarrow GL_2(\mathcal{O}_{K_\beta})$$

(impar, irreducible) para la cual se sabe que la correspondiente reducción módulo p que denotamos $\bar{\rho}$ es o bien reducible o bien modular, lo segundo significa que admite algún "levantamiento" $\hat{\rho}$ que viene dado a una forma propia de Hecke f, es decir: $\hat{\rho} = \rho_{f,\beta'}$

es modular y su reducción módulo β' es isomorfa a $\bar{\rho}$.

En otras palabras, si miramos las trazas a_ℓ de los generadores Frob ℓ de $G_{\mathbb{Q}}$ en la imagen de $\hat{\rho}$ y las trazas b_ℓ para el caso de $\hat{\rho} = \rho_{f,\beta'}$ (que son iguales a los autovalores de f) se tiene:

$$a_\ell \equiv b_\ell \pmod{\beta}, \quad \forall \ell \text{ coprimo con } p \text{ y } N = \mathrm{cond}(\hat{\rho}).$$

Con esta hipótesis de que $\hat{\rho}$ es "residualmente reducible o modular", sumada a otras condiciones técnicas (condiciones locales, tipo de imagen) los teoremas "tipo Wiles" prueban que $\hat{\rho}$ es modular, es decir, que existe $g \in S_k^{new}(N')$ con: $\hat{\rho} \simeq \rho_{g,\beta''}$.

Observación: En el caso $\hat{e}$ residualmente reducible, el único teorema de este tipo del que se disponía hasta hace un par de años es de Skinner y Wiles (1999), y requiere entre otras hipótesis que $\hat{e}$ sea (localmente en p) ordinaria.

El teorema de L. Pan que mencionaremos al acabar renueva esta cuestión en este caso, siendo por lo tanto mucho más versátil.

(2) Este teorema de Taylor (2008) se aplica tanto a una representación a valores en k cuerpo finito, llamémosla $\bar{\rho}$, o a una repr. p-ádica $\hat{\rho}$ de $G_{\mathbb{Q}}$ (bajo ciertas condiciones locales y de la imagen, continua) y pruebo bajo una ingeniosa aplicación de un teorema de Moret-Bailly sobre existencia de puntos en variedades y una aplicación de (1) un resultado de modularidad potencial, es decir, dado $\bar{\rho}$ o $\hat{\rho}$ con ciertas condiciones, pruebo que existe un cuerpo de números F (no controlado!) totalmente real y tal que por split en $F/\mathbb{Q}$ para el cual la restricción $\bar{\rho}|_{G_F}$ o $\hat{\rho}|_{G_F}$ es modular, es decir, es (la reducción módulo $\mathfrak{p}$ o no) una repr. $\mathfrak{p}$-ádica asociada a una forma de Hilbert sobre F ((Snowden, Blasius-Rogawski, Taylor, ...)

Estrategia para la demostración de la conjetura de Serre
(D., Khare-Wintenberger):

Deducir, a partir de (2), las siguientes propiedades para una representación
$\bar{\rho}: G_{\mathbb{Q}} \to GL_2(k)$.

(a) Como $\bar{\rho}|_{G_F}$ es modular para algún cuerpo F, para cierta restricción a G_F se pueden aplicar generalizaciones del resultado de level-lowering de Ribet y concluir que $\bar{\rho}$ admite un levantamiento minimal p-ádico $\tilde{\rho}$ modular, sabiendo además que F y $\tilde{\rho}$ es Hilbert-modular, tiene el peso y el nivel predichos por Serre.

A partir de aquí, combinando con un estudio previo realizado por Böckle sobre el anill. R_{min} de "deformaciones minimales" de $\bar{\rho}$ (concretamente: Böckle establece por métodos puramente Galoisianos que $\dim \mathrm{Krull}(R_{min}) \geq 1$), se deduce que $\bar{\rho}$ admite un levantamiento minimal p-ádico $\hat{\rho}: G_{\mathbb{Q}} \to GL_2(\mathcal{O}_{\overline{a_p}})$:

este $\hat{\rho}$ no se sabe (aún!!) que sea modular, pero posee también un "nivel" (su conductor de Artin: la parte prima con p) y un

"pero" (es cristalino o semiestable, luego es Hodge-Tate con pesos $\{0, k-1\}$) que estarán relacionados (si queremos: serán iguales) los pedidos por Serre.

(b)

Partimos ahora de una representación p-ádica como la

$\hat{e} : G_{\mathbb{Q}} \longrightarrow GL_2(\overline{\mathbb{Q}}_p)$ obtenida en (a), supondremos que es cristalina, cristalina o semiestable en p (o potencialmente_) y que cumple las condiciones técnicas necesarias para la aplicación de las herramientas (1) y (2) de Wiles y Taylor.

Por (2), tenemos que para un cierto cuerpo F: $\hat{e}|_{G_F}$ es Hilbert-modular. Además se puede escoger $F/\mathbb{Q}$ Galois.

Entonces, por cambio de base resoluble (Langlands), para todo cuerpo intermedio $\mathbb{Q} \subseteq F' \subseteq F$ con $Gal(F/F')$ resoluble, también se tiene: $\hat{e}|_{G_{F'}}$ Hilbert-modular.

A partir de aquí siguiendo el formalismo de Brauer, se puede construir, para todo primo $l \neq p$, partiendo de las representaciones l-ádicas asociadas a las formas de Hilbert h_i sobre F' una representación virtual de $G_{\mathbb{Q}}$: para el caso $l = p$ esta representación tiene que coincidir con $\hat{e}$ pues las restricciones de $\hat{e}|_{G_{F'}}$ son las representaciones $e_{h_i, 0}$

De aquí puede verse, basándose en que para cada $F_{(\ell)}$ los sistemas de representaciones $\{\rho_{h,\ell}\}_{\ell \in P}$ son compatibles, y utilizando resultados de representaciones de grupos, que para todo ℓ la representación virtual ℓ-ádica de $G_{\mathbb{Q}}$ obtenida "pegando" los $\rho_{h,\ell}$ es una representación de Galois genuina, 2-dimensional, e irreducible, y por construcción es compatible con $\hat{e}$: Es decir: hemos probado que tal como ocurre para el caso de una $\rho_{E/P}$ asociada a una curva elíptica o una $\rho_{f,\beta}$ asociada a una forma modular, para una representación $\hat{e}$ p-ádica con buenas propiedades locales, siempre existe un sistema compatible $\hat{e} \subseteq \{\rho_\ell\}$ que la contiene: todos los ρ_ℓ tendrán el mismo "nivel" (= conductor) y para todo ℓ fuera del conductor de $\hat{e}$ serán cristalinos.

Todos serán (pol.) cristalinos o semicristalinos, Hodge-Tate con números constantes $\{0, k-1\}$ iguales a los de $\hat{e}$.

Demostración: Versión Simplificada:

gracias al teorema de L. Pan, podemos presentar una versión simplificada de la demostración: La versión "actual" es muy sencilla, se aplican los resultados (a) y (b) anteriores hasta reducir peso, nivel y característica hasta valores muy pequeños donde se tiene reducibilidad residual por resultados de Tate y Serre, y desde aquí se propaga la modularidad "backwards" gracias a los teoremas tipo Wiles (a).

Esquemáticamente: $\rho : G_{\mathbb{Q}} \to GL_2(k)$ en característica $p>2$ con nivel de Serre $N(\rho)=N$: por simplicidad suponemos N impar y:

$S = \{p_1, \dots, p_r\}$ = primos que dividen a N.

Por (a) ρ admite un levantamiento $\mathbb{Q}$-sdio $\hat{\rho}$ con "nivel" N y pesos Hodge-Tate $\{0, k(\ell)-1\}$, además $\hat{\rho}$ es cristalino.

Construimos mediante (b) el sistema compatible $\hat{\rho} \subseteq \{\hat{\rho}_\ell\}$.

Nos detenemos en p_1: $\hat{\rho}_{p_1} \subseteq \{\hat{\rho}_\ell\}$: al reducir módulo p_1, la representación residual ρ_{p_1}, por definición, tiene un primo menos en el nivel.

Iterando este procedimiento (se aplica luego a p_2, ... y así hasta p_r) acabamos en: $\rho_{p_r} : G_{\mathbb{Q}} \to GL_2(k')$ k' de característica p_r, con nivel $N(\rho_{p_r})=1$.

Esto ya reduce la demostración de la conjetura al caso $N=1$:

pues si ρ_ℓ es modular, por los teoremas (1) $\hat{\rho}_\ell$ también, luego el sistema que lo contiene también, y así retrocediendo con teoremas tipo (1) hasta llegar a $\hat{\rho}$ y ρ modulares.

Aquí hemos supuesto que en todos los pasos el reducir módulo $p_1, p_2, \ldots, p_r$ los reps. residuales son (abs.) irreducibles.

Caso contrario: El teorema de L. Pan / Skinner-Wiles implica la modularidad del levantamiento (nos hemos detenido en el primer p_i tal que ρ_{p_i} es reducible) desde donde retrocedíamos como antes se llega a la modularidad de ρ.

Una vez en nivel 1: También aquí el teo de Pan permite acabar rápidamente (hay que evitar $p=3$ pero para simplificar la prueba obvio este tecnicismo): Si $\rho : G_{\mathbb{Q}} \to GL_2(k)$ es de nivel 1, su levantamiento mínimo como en (a) $\hat{\rho}$ tiene nivel $\neq 1$, y la familia o sistema $\hat{\rho} \subseteq \{\hat{\rho}_\ell\}$ que lo contiene es de nivel 1. Entonces para $\ell=3$, la representación modulo 3 ρ_3 será de $N(\rho_3)=1$, es decir, no ramificada fuera de 3. En este caso, y fue maravilloso cuando descubrí en 2003 este guantazo inicial debido al propio Serre,

Serre menciona en el Vol. IV de sus Obras que ya en 1973 observó que un resultado probado por Tate para $p=2$ funciona con igual prueba para $p=3$ y prueba que una repr:

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

en característica 3 con $N(\rho)=1$ tiene que ser reducible.
(utilizan los cotas de Odlyzko para root discriminant... nada de modularidad aún!)

Luego estamos en condiciones de aplicar el teo. de Ribet
(cuando apliqué esto allá por 2004 a conjetura de Serre por primera vez sólo trate los casos $k(\rho)=2$ y $k(\rho)=4$ donde puede probarse que $\hat{\rho}$ ha de ser ordinaria pues ρ es reducible y aplicar entonces el (teorema tipo (1) de Skinner-Wiles) y concluir que

$\hat{\rho}_3$ es modular, luego el sistema $\{\hat{\rho}_\ell\}$ es modular,

luego $\hat{\rho}$ es modular y por lo tanto,

reducida módulo 3, ρ es modular

(Obs: como actualmente hay aún algunas condición técnica para $p=3$ en el teo. de Ribet, en realidad de momento hay que coger $\ell=5$ y aplicar una variante de Schoof al resultado de Tate-Serre como "caso base".