Seminario de modularidad de representaciones de Galois (2020-1)

Héctor Pastén

Pontificia Universidad Católica de Chile

2020/05/12

Contenido de hoy:

Curvas elípticas modulares

- Caso base: las que vienen de la construcción de Shimura.
- Caso general: isógenas a las anteriores.
- Formulaciones equivalentes: $L(E, s) = L(f, s)$, etc.
- Ejemplo.

Repaso: construcción de Shimura

Fijamos N y un grupo $\Gamma_1(N) \subseteq \Gamma \subseteq \Gamma_0(N)$.

- Sea $f \in S_2(\Gamma)$ una newform de nivel N: $f = q + a_2(f)q^2 + \ldots \in S_2(\Gamma)$.
- Sea $O_f = \mathbb{Z}[a_n(f) : n \geq 1]$ y $K_f = \mathbb{Q}(a_n(f) : n \geq 1)$. Obtenemos un morfismo de anillo $\lambda_f : \mathbb{T}_{\mathbb{Z}} \to K_f$.
- Definimos $\mathcal{I}_f = \ker(\lambda_f) \subseteq \mathbb{T}_{\mathbb{Z}}$.
- $\mathbb{T}_{\mathbb{Z}}$ actúa en J_Γ, y esa acción es con endomorfismos definidos sobre $\mathbb{Q}$ gracias a la interpretación modular.
- En particular $\mathcal{I}_f \cdot J_\Gamma$ es una sub-variedad abeliana de J_Γ definida sobre $\mathbb{Q}$: es subgrupo, y es conexa porque $0 \in t \cdot J_\Gamma$ para todo $t \in \mathbb{T}_{\mathbb{Z}}$.
- Se define $A_f := J_\Gamma / \mathcal{I}_f \cdot J_\Gamma$. Es una variedad abeliana definida sobre $\mathbb{Q}$. Cumple $\dim A_f = [K_f : \mathbb{Q}]$ (cálculo en $Tan_0(J_\Gamma^{an}) \simeq S_2(\Gamma)$).
- A_f adquiere una estructura de O_f-módulo, y por ende, de $\mathbb{T}_{\mathbb{Z}}$-módulo via λ_f. Con esta acción, el cuociente $p_f : J_\Gamma \to A_f$ es $\mathbb{T}_{\mathbb{Z}}$-equivariante.

Repaso: aritmética de A_f

Notación: $B/\mathbb{Q}$ variedad abeliana, ℓ primo. $T_\ell(B) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell =: V_\ell(B)$.

- Obtenemos un morfismo $p_{f,*} : V_\ell(J_\Gamma) \to V_\ell(A_f)$ que es
  - $G_\mathbb{Q}$-equivariante, y
  - $\mathbb{T}_{\mathbb{Q}_\ell}$-equivariante.
- Como $V_\ell(J_\Gamma)$ es libre de rango 2 sobre $\mathbb{T}_{\mathbb{Q}_\ell}$ obtenemos **Corolario.** $V_\ell(A_f)$ es libre de rango 2 sobre $K_f \otimes \mathbb{Q}_\ell$.
- Si $p \nmid N$ entonces X_Γ tiene buena reducción en p, y por ende J_Γ también. Como A_f es cuociente de J_Γ, también tiene buena reducción.
- **Teorema.** (Corolario de Eichler-Shimura) Si $p \nmid N\ell$, entonces el polinomio característico de *Frob* en $V_\ell(J_\Gamma)$ visto como $\mathbb{T}_{\mathbb{Q}_\ell}$-módulo (libre de rango 2) es $X^2 - T_p X + p\langle p \rangle$.

Repaso: aritmética de A_f

- **Teorema.** $(p \nmid N\ell)$ Sea ψ el nebentypus de f. Tenemos que

$$\#A_f(\mathbb{F}_p) = Nr_{K_f/\mathbb{Q}}\left(1 - a_p(f) + \psi(p)p\right).$$

  En particular, si $K_f = \mathbb{Q}$ (i.e. A_f curva elíptica) entonces $a_p(f) = a_p(A_f)$.

- **Teorema.** Sea f newform de nivel N. Entonces A_f tiene conductor $N^{\dim A_f} = N^{[K_f:\mathbb{Q}]}$ y su función L cumple

$$L(A_f, s) = \prod_{g \in [f]} L(g, s).$$

  En particular, $L(A_f, s)$ tiene ecuación funcional y continuación analítica.

Aplicación: cotas para $|a_p(f)|$

Teorema. Sea $f \in S_2(\Gamma_0(N))$ newform. Entonces para todo $p \nmid N$ se tiene

$$|a_p(f)| \leq 2\sqrt{p}$$

Dem. Comparando factores de Euler en p se tiene

$$det(1 - FX|\mathcal{V}_\ell(A_f)) = \prod_{\sigma: K_f \to \mathbb{C}} (1 - a_p(f)^\sigma X + pX^2)$$

Para explicar la idea, voy a suponer $K_f = \mathbb{Q}$ (A_f curva elíptica). En este caso escribimos α_p, β_p por los valores propios de F y se obtiene

$$(1 - \alpha_p X)(1 - \beta_p X) = 1 - a_p(f)X + pX^2$$

Deducimos $|a_p(f)|_{\mathbb{C}} = |\alpha_p + \beta_p|_{\mathbb{C}} \leq 2p^{1/2}$ por la cota de Hasse.
En el caso general los $2[K_f : \mathbb{Q}]$ valores propios de F actuando en $\mathcal{V}_\ell(A_f)$ también tienen módulo complejo $p^{1/2}$, por un teorema de Weil.

Ejemplo: congruencias

Supongamos que la newform $f \in S_2(\Gamma_0(N))$ cumple que $K_f = \mathbb{Q}$ y que A_f es una curva elíptica con un punto racional de orden 2. ¿Qué consecuencia tendría eso para f?

- Si $p \nmid 2N$ entonces $\#A_f(\mathbb{F}_p)$ es par porque $A_f(\mathbb{F}_p)$ tiene un subgrupo isomorfo a $A_f(\mathbb{Q})[2]$ (teorema de la inyectividad en torsión para buena reducción).
- Entonces

$$a_p(f) = a_p(A_f) = p + 1 - \#A_f(\mathbb{F}_p) \equiv p + 1 \equiv 0 \bmod 2$$

  para todo $p \nmid 2N$.

¿Cómo se ve f mod 2?

Curvas elípticas modulares fuertes

Una curva elíptica E es *modular fuerte* (o "strong Weil curve", u "optimal modular elliptic curve") si es isomorfa a una A_f que viene de la construcción de Shimura aplicada a una newform f con $K_f = \mathbb{Q}$.

Lema. Si E es una curva elíptica modular fuerte de conductor N, entonces $E \simeq A_f$ con $f \in S_2(\Gamma_0(N))$ newform.

Dem. Por el resultado anterior sobre funciones L y conductores, tenemos que f es newform de nivel N. Como $K_f = \mathbb{Q}$ tenemos que el nebentypus es trivial así que $f \in S_2(\Gamma_0(N))$. □

Curvas elípticas modulares

Una curva elíptica E es *modular* si es isógena sobre $\mathbb{Q}$ a una curva elíptica modular fuerte A_f. Ambas E y A_f tiene el mismo conductor (son isógenas) que coincide con el nivel de la newform $f \in S_2(\Gamma_0(N))$.

Teorema. Sea $E/\mathbb{Q}$ curva elíptica de conductor N. Son equivalentes:

- (Mod. Isogenia) E es isógena sobre $\mathbb{Q}$ a una curva elíptica modular fuerte A_f.
- (Mod. Curvas) Existe un morfismo no-constante $\phi : X_0(N) \to E$ definido sobre $\mathbb{Q}$.
- (Mod. L) Existe una newform $f \in S_2(\Gamma_0(N))$ con $K_f = \mathbb{Q}$ que cumple $L(E, s) = L(f, s)$.
- (Mod. Galois) Existe una newform $f \in S_2(\Gamma_0(N))$ con $K_f = \mathbb{Q}$ tal que para **algún** primo ℓ se cumple que las representaciones de Galois $\rho_{E,\ell} : G_{\mathbb{Q}} \to \mathcal{V}_\ell(E)$ y $\rho_{A_f,\ell} : G_{\mathbb{Q}} \to \mathcal{V}_\ell(A_f)$ son isomorfas.

Además, en (MC) se cumple que $\phi^* \omega_E = c \cdot f(z)dz$ para algún $c \neq 0$.

Curvas elípticas modulares

- $MI \to MC$: Componer $X_0(N) \to J_0(N) \to A_f \to E$. Es no-constante porque el pull–back de un diferencial da un múltiplo no-nulo de $f(z)dz$; ver nuestro análisis de $Tan_0(A_f) \simeq S_f = \mathbb{C} \cdot f$.
- $MC \to MI$: $X_0(N) \to E$ induce un morfismo no-constante $J_0(N) \to E$. Entonces E es un factor isógeno de $J_0(N)$. Los A_g para g newfor m son simples sobre $\mathbb{Q}$, así que ese factor debe ser un A_f completo.
- $MI \to ML$: MI implica que $\mathcal{V}_\ell(E) \simeq \mathcal{V}_\ell(A_f)$ para cada ℓ. Viendo la definición de la función L obtenemos ML.

Curvas elípticas modulares

- $ML \to MG$: La teoría analítica de números nos da que una serie de Dirichlet $D(s) = \sum_n b_n/n^s$ que converge en un semi-plano no vacío determina de forma única los b_n. Entonces $a_p(E) = a_p(f) = a_p(A_f)$ para todo primo p. Esa igualdad de trazas de Frobenius, por Chebotarev, muestra que $tr(\rho_{E,\ell}) = tr(\rho_{A_f,\ell})$. Son representaciones semisimples así que son isomorfas por Brauer-Nesbitt.
- $MG \to MI$: Esta es un caso de la *conjetura de Tate* demostrado por Faltings (antes, por Serre para curvas elípticas salvo el caso CM). aka Teorema de la isogenia.

En resumen, demostramos: $MC \leftrightarrow MI \to ML \to MG \to MI$. □

Conjetura de Taniyama-Shimura-Weil

Conjetura TSW (Taniyama, 1955 en un proceedings de conferencia). Toda curva elíptica sobre $\mathbb{Q}$ es modular en el sentido de funciones L.

- Gauss ($\sim$1800) demostró un resultado que en lenguaje moderno demuestra esta conjetura para las curvas elípticas $y^2 = x^3 - x$, $x^3 + y^3 = 1$ y twists de ellas.
- Varios trabajos: Hecke-Deuring (caso CM), Weil ("converse theorem": función L analíticamente decente implica modularidad), Eichler y Shimura (construcción de la clase de hoy).
- (1995) Andrew Wiles y R. Taylor - A. Wiles demostraron esta conjetura para todas las curvas elípticas semi-estables (conductor libre de cuadrados).
- (2001) C. Breuil, B. Conrad, F. Diamond, R. Taylor terminaron de demostrar completamente la conjetura TSW en su artículo "Wild 3-adic exercises".

Conjetura de Taniyama-Shimura-Weil

Gracias a [W,TW, BCDT] finalmente se tiene:
Teorema de modularidad. Toda curva elíptica sobre $\mathbb{Q}$ es modular.

Esto tiene una serie de profundas consecuencias.

- FLT
- Bases de datos exhaustivas de curvas elípticas.
- Excelentes propiedades analíticas de $L(E, s)$.
- Grandes avances en BSD.
- Una manera de atacar la conjetura *abc*.
- etc.
- La demostración dio una técnica para obtener modularidad de muchos otros objetos matemáticos, lo que lleva a una serie de otros resultados de este calibre no solo para curvas elípticas.