Modularidad de curvas elípticas semiestables

Natalia García

24 de julio de 2020

Ayer

Notación: $\ell > 2$ primo. $K/\mathbb{Q}_\ell$ finita.

Teorema 1 (Modularity lifting)

Sea $\rho : G_{\mathbb{Q}} \to GL_2(K)$ representación continua, y $\bar{\rho}$ su reducción. Si

1. *$\bar{\rho}$ es irreducible y modular,*
2. *$\rho_{|I_p} \sim \left(\begin{smallmatrix} 1 & \star \\ 0 & 1 \end{smallmatrix}\right)$ para todo $p \neq \ell$,*
3. *$\rho_{|G_\ell}$ es semiestable,*
4. *$\det\rho = \epsilon$,*

entonces ρ es modular.

Modularidad para algunas curvas elípticas semiestables

Teorema 2

Si $E/\mathbb{Q}$ es una curva elíptica semiestable tal que $\bar{\rho}_{E,3}$ es irreducible, entonces E es modular.

Dem: Recordamos que E es modular si $\rho_{E,3}$ es modular.

Aplicamos Teorema 1 con $\ell = 3$:

1. $\bar{\rho}_{E,3}$ es irreducible por hipótesis,
2. $\rho_{E,3|I_p} \cong \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$ para $p \neq 3$,
3. $\rho_{E,3}$ semiestable, pues E es semiestable,
4. $\det\rho_{E,3} = \epsilon$.

1. $\bar{\rho}_{E,3}$ es modular por:

Teorema 3 (T2.13 de DDT)

Sea $\bar{\rho} : G_{\mathbb{Q}} \to GL_2(k)$ una representación continua absolutamente irreducible con $\det(\bar{\rho}(c)) = -1$. Suponer que se cumplen

(a) $k = \mathbb{F}_3$,

(b) *la imagen proyectiva de $\bar{\rho}$ es diedral.*

Entonces $\bar{\rho}$ es modular.

Como se cumplen todas las condiciones del Teorema 1, obtenemos que E es modular.

Taniyama-Shimura para curvas elípticas semiestables

Le quitaremos una hipótesis al teorema anterior.

Teorema 4

Si $E/\mathbb{Q}$ es una curva elíptica semiestable, entonces E es modular.

Recordando que E modular es lo mismo que $\rho_{E,\ell}$ modular para algún ℓ, nos basta encontrar un ℓ donde esto ocurra.

Cuando $\bar{\rho}_{E,3}$ es irreducible, sabemos que $\rho_{E,3}$ es modular. Nos falta estudiar el caso $\bar{\rho}_{E,3}$ reducible.

Lema 1

Sea $E/\mathbb{Q}$ semiestable con $\bar{\rho}_{E,3}$ reducible. Entonces $\bar{\rho}_{E,5}$ es irreducible.

Dem: Como $\bar{\rho}_{E,3}$ es reducible, E tiene un subgrupo de orden 3 definido sobre $\mathbb{Q}$. Si $\bar{\rho}_{E,5}$ fuera reducible, entonces E tiene un subgrupo de orden 15 definido sobre $\mathbb{Q}$.

Por interpretación modular, obtenemos un punto racional no cuspidal en la curva $X_0(15)$.

La curva $X_0(15)$ no tiene puntos racionales no cuspidales asociadas a curvas elípticas semiestables. Por lo tanto $\bar{\rho}_{E,5}$ es irreducible.

Sabemos entonces, que cuando $\bar{\rho}_{E,3}$ es reducible:

1. $\bar{\rho}_{E,5}$ es irreducible,
2. $\rho_{E,5|I_p} \cong \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$ para $p \neq 5$,
3. $\rho_{E,5}$ semiestable,
4. $\det \rho_{E,5} = \epsilon$.

Para aplicar Teorema 1, sólo nos falta mostrar que $\bar{\rho}_{E,5}$ es modular.

Lema 2

Existe una curva elíptica semiestable $A/\mathbb{Q}$ que cumple

(a) $A[5] \cong E[5]$ *como* $G_{\mathbb{Q}}$*-módulos,*

(b) $A[3]$ *es un* $G_{\mathbb{Q}}$*-módulo irreducible.*

Dem: Consideramos el funtor

$$F_{E[5]}(L) = \left\{ (A/L, \alpha) : \begin{array}{c} A \text{ curva elíptica, con } E[5] \xrightarrow{\alpha} A[5] \\ \text{isom. respetando pairing de Weil} \end{array} \right\}.$$

Por Katz-Mazur "Arithmetic moduli of elliptic curves", existe una curva $Y'/\mathbb{Q}$ que lo representa. Sea X' su compactificación.

La curva modular $X(5)$ representa el funtor

$$F_5(L) = \left\{ (A/L, \alpha) : \begin{array}{c} A \text{ curva elíptica, con } \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \xrightarrow{\alpha} A[5] \\ \text{isom. respetando pairing de Weil} \end{array} \right\}$$

Por la definición de los funtores, las curvas $X'/\mathbb{C}$ y $X(5)/\mathbb{C}$ son isomorfas.

Sabemos que $g(X(5)) = 0$ así que X' es de género 0.

Por otra parte, X' tiene un punto racional definido sobre $\mathbb{Q}$, asociado a $A = E$, así que $X'/\mathbb{Q}$ tiene infinitos puntos racionales, por lo tanto hay infinitas curvas elípticas $A/\mathbb{Q}$ que cumplen $A[5] \cong E[5]$.

Para estudiar (b), consideramos

$$F_{5,3}(L) = \left\{ (A/L, \alpha) : \begin{array}{c} A \text{ curva elíptica, con } E[5] \xrightarrow{\alpha} A[5] \text{ isom. respetando} \\ \text{pairing de Weil, y } G < A \text{ de orden } 3 \end{array} \right\}.$$

Existe una curva Y'' representando este funtor. Esta curva tiene género 9, calculado con Magma:

```
G := Intersection(CongruenceSubgroup(5),CongruenceSubgroup(0,3));
G;
Genus(G)
```

Por el teorema de Faltings para curvas, obtenemos que $Y''/\mathbb{Q}$ contiene solamente finitos puntos racionales.

A partir de las definiciones de $F_{5,3}$ y $F_{E[5]}$, tenemos una función

$$Y'' \to Y'$$

definida sobre $\mathbb{Q}$. Solo finitos puntos racionales de Y' vienen de Y'', así que obtenemos infinitas curvas elípticas A con un subgrupo G definido sobre $\mathbb{Q}$ de orden 3, así que cumpliendo (b).

Nos falta mostrar que A es semiestable. Usamos "Fermat's Last Theorem: basic tools", Takeshi Saito. Como $A[\ell] \cong E[\ell]$, la curva E es semiestable y $\ell \geq 5$, tenemos que A es semiestable para $p \neq \ell$.

Por otra parte, dado $x_E \in Y'$, como $Y' \cong \mathbb{P}^1$ sobre $\mathbb{Q}$ podemos elegir $x_A \in Y'$, suficientemente cercano a x_E en la topología 5-ádica, para que $\rho_{E,5|G_5}$ semiestable implique $\rho_{A,5|G_5}$ semiestable.

Como $\rho_{A,5}$ es semiestable para todo p, obtenemos que $\rho_{A,5}$ es semiestable.

Demostración de Taniyama-Shimura

Como A es semiestable y su representación $\bar{\rho}_{A,3}$ es irreducible, obtenemos por Teorema 2 que A es modular, así que $\rho_{A,5}$ es modular.

Por lo tanto $\bar{\rho}_{A,5} \cong \bar{\rho}_{E,5}$ es modular.

Por Teorema 1 obtenemos finalmente que $\rho_{E,5}$ es modular, así que E es modular.

Último teorema de Fermat

Teorema 5

Sea $n \geq 3$ entero. La ecuación $x^n + y^n = z^n$ no tiene soluciones enteras con $xyz \neq 0$.

Por contradicción, suponemos que hay una solución a, b, c.

- Podemos suponer que a, b, c son coprimos.
- Los casos $n = 3, 4, 5, 7$ se conocen desde la antigüedad.
- Podemos suponer que $n = \ell$ con $\ell > 7$ es primo.

Consideramos la curva elíptica de Frey

$$E : y^2 = x(x - a^\ell)(x + b^\ell)$$

Es semiestable y su discriminante minimal es $\Delta_E = 2^{-8}(abc)^{2\ell}$.

Como es semiestable, es modular.

Como $\ell > 7$ y E es semiestable, la representación $\bar{\rho}_{E,\ell}$ es absolutamente irreducible (Mazur).

Finalmente notamos que para todo $p \neq 2$, se cumple $\ell \mid v_p(\Delta_E)$.

Podemos usar level-lowering:

Teorema 6 (T3.15 en DDT)

Suponer que $\ell > 3$ y $\bar{\rho}$ es absolutamente irreducible y modular. Entonces existe una newform f de peso 2 tal que

1. $\bar{\rho} \cong \bar{\rho}_f$,
2. $N_f = N(\bar{\rho})\ell^{\delta(\bar{\rho})}$.

Consideramos $\bar{\rho} = \bar{\rho}_{E,\ell}$. Obtenemos una newform $f \in S_2(\Gamma_1(N_f))$.

Aquí $N_f = \ell^{\delta(\bar{\rho})} N(\bar{\rho})$ donde $N(\bar{\rho}) = \prod_{p \neq \ell} p^{m_p(\bar{\rho})}$.

Usando Prop 2.12 [DDT] calculamos los números que aparecen en $N_f = \ell^{\delta(\bar{\rho})} N(\bar{\rho})$ donde $N(\bar{\rho}) = \prod_{p \neq \ell} p^{m_p(\bar{\rho})}$.

1. $m_2 = 0$ o 1 porque E es semiestable,
2. $m_p = 0$ para todo $p \neq 2, \ell$, porque E es semiestable y $\ell | v_p(\Delta_E)$,
3. $\delta = 0$ porque E es semiestable y $\ell | v_\ell(\Delta_E)$.

Por lo tanto $N_f = 1$ o 2.

Pero $S_2(\Gamma_1(1)) = 0$ y $S_2(\Gamma_1(2)) = 0$, así que f no puede existir. Contradicción. □