Variedades modulares: Resultados y conjeturas de finitud

MAT.ES 2005

Víctor Rotger

1. CURVAS ELÍPTICAS SOBRE CUERPOS DE NÚMEROS

$K \subset \bar{\mathbb{Q}}$ cuerpo de números

$E/K : y^2z = x^3 + axz^2 + bz^3, \quad a, b \in K, 4a^3 + 27b^2 \neq 0$
es una variedad abeliana de dimensión 1 sobre K:

- $O := [0 : 1 : 0] \in E(K)$
- $+ : E \times E \longrightarrow E$ (Regla de la secante-tangente)
- $i : E \longrightarrow E$

Dada E/K, estamos interesados en:

- La torsión de E: $E(K)_{\text{tors}} = \{P \in E(K) : N \cdot P = O, N \geq 1\}$.
- Los anillos de endomorfismos $\mathrm{End}_K(E), \quad \mathrm{End}_{\bar{\mathbb{Q}}}(E)$.
- Si $K = \mathbb{Q}$, la modularidad de E.

Teorema de Mordell-Weil. Sea K un cuerpo de números. Entonces

$$E(K) \simeq \mathbb{Z}^r \times T,$$

donde $r \geq 0$, $T = E(K)_{tors}$ un grupo finito.

Conjetura. Sea K un cuerpo de números. Para todo $r_0 \geq 0$, existe una curva elíptica E/K tal que

$$r = \text{rango } E(K) \geq r_0.$$

Ejemplo (Martin-McMillen). Existe una curva elíptica $E/\mathbb{Q}$ con *rango* $E(\mathbb{Q}) \geq 24$.

Resultados de finitud sobre la torsión.

Teorema (B. Mazur). Si $N > 12$, no existe $E/\mathbb{Q}$ con $P \in E(\mathbb{Q})$, $\mathrm{ord}(P) = N$.

Teorema (L. Merel). Sea $d \geq 1$. Existe $N_d \geq 1$ tal que para todo $N > N_d$:

$$\nexists\, E/K, [K : \mathbb{Q}] \leq d, \text{ con } P \in E(K), \mathrm{ord}(P) = N.$$

P. Parent calcula explícitamente N_d para cada $d \geq 1$.

Resultados de finitud sobre los endomorfismos.

Teorema. Sea K un cuerpo de números. Hay un número finito de $\mathbb{Q}$-álgebras B para las que existe E/K tal que

$$\mathrm{End}^0_{\bar{\mathbb{Q}}}(E) := \mathbb{Q} \otimes \mathrm{End}_{\bar{\mathbb{Q}}}(E) \simeq B.$$

Demostración. Por la teoría de Shimura-Taniyama, $\mathrm{End}^0_{\bar{\mathbb{Q}}}(E) \simeq \mathbb{Q}$ o $F = \mathbb{Q}(\sqrt{-d})$, $d > 0$, con $h(F) \leq [K : \mathbb{Q}]$. Por el teorema de Siegel, la desigualdad se cumple solo para un número finito de cuerpos F.

Ejemplo. Si $E/\mathbb{Q}$, entonces $\mathrm{End}^0_{\bar{\mathbb{Q}}}(E) \simeq \mathbb{Q}$ o $\mathbb{Q}(\sqrt{-d})$ para $d = 1, 2, 3, 7, 11, 19, 43, 67$ o 163.

Modularidad de curvas elípticas sobre $\mathbb{Q}$

Definición. Una curva elíptica $E/\mathbb{Q}$ es modular si existe un morfismo exhaustivo definido sobre $\mathbb{Q}$

$$\pi : X_1(N) \longrightarrow E$$

para algún $N \geq 1$.

Teorema (A. Wiles et al.) Toda curva elíptica $E/\mathbb{Q}$ es modular.

2. CURVAS MODULARES Y CURVAS DE SHIMURA

- $B_D = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij$, $i^2 = a, j^2 = b, ij = -ji$ con $a, b \in \mathbb{Q}^*$, a ó $b > 0$, álgebra de cuaterniones indefinida.
- $D = \mathrm{disc}(B) = p_1 \cdots p_{2r}$, donde $B \otimes \mathbb{Q}_{p_i} \not\simeq \mathrm{M}_2(\mathbb{Q}_{p_i})$.
- $N \geq 1$, $(D, N) = 1$.
- $\mathcal{O}_{D,N} \subseteq B$ anillo de enteros localmente maximal en $p \nmid N$ y tal que $\mathcal{O} \otimes \mathbb{Z}_p \simeq \{A \in \mathrm{M}_2(\mathbb{Z}_p), A \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mod p^f\}$ en $p^f \mid\mid N$.
- $\Gamma_1(D, N) = \{\gamma \in \mathcal{O}^*_{D,N}, \det(\gamma) = 1\} \subset \mathrm{SL}_2(\mathbb{R})$

La curva de Shimura de discriminante $D = p_1 \cdots p_{2r}$ y nivel N, $(D, N) = 1$, sobre $\mathbb{C}$ es

$$X_1(D, N)_{\mathbb{C}} := \Gamma_1(D, N) \backslash \mathcal{H}^*, \quad \mathcal{H}^* = \{\tau \in \mathbb{C}, \mathrm{Im}(\tau) > 0\} \cup \mathbb{P}^1(\mathbb{Q}).$$

Teorema (Shimura). La superfície de Riemann $X_1(D, N)_{\mathbb{C}}$ admite un modelo canónico $X_1(D, N)/\mathbb{Q}$.

Notación:
Si $D = 1$, $X_1(N) := X_1(D, N)$, curva modular clásica.
Si $N = 1$, notamos $X_D := X_1(D, 1)$.

Definiciones equivalentes de modularidad

Una curva elíptica $E/\mathbb{Q}$ es modular si:

1. $\exists \quad \pi : X_1(N) \overset{/\mathbb{Q}}{\twoheadrightarrow} E$ para algún $N \geq 1$.

2. $\exists \quad \pi : \mathrm{Jac}(X_1(N)) \overset{/\mathbb{Q}}{\twoheadrightarrow} E$ para algún $N \geq 1$.

3. $\exists \quad \pi : X_1(D, N) \overset{/\mathbb{Q}}{\twoheadrightarrow} E$ para algún $D = p_1 \cdots p_{2r}$, $(D, N) = 1$.

1 $\Leftrightarrow$ **2**: Por la propiedad universal de $X_1(N) \hookrightarrow \mathrm{Jac}(X_1(N))$,
$\pi : X_1(N) \twoheadrightarrow E$ se extiende a $\pi^* : \mathrm{Jac}(X_1(N)) \twoheadrightarrow \mathrm{Jac}(E) \simeq E$.

2 $\Leftrightarrow$ **3**: $\mathrm{Jac}(X_1(D, N)) \hookrightarrow \mathrm{Jac}(X_1(DN))$.

Interpretación modular de la conjetura de finitud de torsiones de curvas elípticas:

$\exists\, E/K$ con $P \in E(K), \mathrm{ord}(P) = N \quad \Leftrightarrow \quad \exists\, x \in X_1(N)(K) \backslash \{$ cusps$\}$.

Conjetura. Sea $d \geq 1$. Existe $N_d \geq 1$ tal que

$$X_1(D, N)(K) \setminus \{ \text{ cusps, CM } \} = \emptyset$$

para todo $[K : \mathbb{Q}] \leq d$, $D \cdot N > N_d$.

• Por el Teorema de Merel, la conjetura es cierta para $D = 1$.

• Si $D > 1$, $\{$ cusps $\} = \emptyset$ y se conjetura $X_1(D, N)(K) = \{CM\}$ para $[K : \mathbb{Q}] \leq d$, $D \cdot N > N_d$.

3. VARIEDADES ABELIANAS SOBRE CUERPOS DE NÚMEROS

$K \subset \bar{\mathbb{Q}}$ cuerpo de números.
Una variedad abeliana sobre K es una variedad proyectiva A/K dotada de

- $O \in A(K)$
- $+ : A \times A \longrightarrow A$
- $i : A \longrightarrow A$

Teorema de Mordell-Weil. $A(K) \simeq \mathbb{Z}^r \times T, \quad r \geq 0,\ T$ finito.

Torsión y rango

Conjetura. Dados $d, g \geq 1$, existe $N_{d,g}$ tal que para toda A/K de dimensión g, $[K : \mathbb{Q}] \leq d$ y $P \in A(K)$:

$$\mathrm{ord}(P) = N \Rightarrow N \leq N_{d,g}.$$

Conjetura. Dado K y $g \geq 1$, para todo $r_0 \geq 0$, existe una variedad abeliana A/K de dimensión g tal que

$$\text{rango } A(K) > r_0.$$

Dos versiones de modularidad

Una variedad abeliana $A/\mathbb{Q}$ es modular si para algún $N \geq 1$ existe

$$\pi : \mathrm{Jac}(X_1(N)) \overset{/\mathbb{Q}}{\twoheadrightarrow} A.$$

Una curva $C/\mathbb{Q}$ es modular si para algún $N \geq 1$ existe

$$\pi : X_1(N) \overset{/\mathbb{Q}}{\twoheadrightarrow} C.$$

Conjetura de Shimura-Taniyama-Weil. Toda variedad abeliana $A/\mathbb{Q}$ tal que $\mathrm{End}^0_{\mathbb{Q}}(A) = F$, un cuerpo de números F de grado $[F : \mathbb{Q}] = \dim(A)$, es modular.

Conjetura (M. Baker, E. González, J. González, B. Poonen). Dado $g \geq 2$, existe un número finito de curvas modulares de género g.

Modularidad de variedades abelianas

Definición. Una variedad abeliana $A/\mathbb{Q}$ tal que $\mathrm{End}^0_{\mathbb{Q}}(A) = F$, un cuerpo de números F de grado $[F : \mathbb{Q}] = \dim(A)$, se llama *de tipo* GL_2 *sobre* $\mathbb{Q}$.

Teorema (K. Ribet.) Si la Conjetura de Serre sobre la modularidad de representaciones de Galois irreducibles e impares con valores en $\mathrm{GL}_2(\mathbb{F}_q)$ es cierta, toda variedad abeliana A de tipo GL_2 sobre $\mathbb{Q}$ es modular.

Teorema (A. Wiles et al.) Toda curva elíptica $E/\mathbb{Q}$ es modular.

Teorema (J. Ellenberg). Toda superfície abeliana $A/\mathbb{Q}$ de tipo GL_2 sobre $\mathbb{Q}$, con reducción ordinaria en 3 y 5, es modular.

Modularidad de curvas de género ≥ 2

Definición. Una curva $C/\mathbb{Q}$ de género $g \geq 2$ es *modular nueva* si existe

$$\pi : X_1(N) \twoheadrightarrow C$$

tal que

$$\pi^*\Omega^1(C) \subseteq \Omega^1(X_1(N))^{\text{new}},$$

donde

$$\Omega^1(X_1(N)) = \Omega^1(X_1(N))^{\text{old}} \oplus \Omega^1(X_1(N))^{\text{new}}.$$

Teorema (M. Baker, E. González, J. González, B. Poonen). Dado $g \geq 2$, existe un número finito de curvas modulares nuevas de género g.

Cuestión. Sea $g \geq 2$. ¿Existe un número finito de curvas $C/\mathbb{Q}$ de género g para las que

$$X_1(D, N) \twoheadrightarrow C,$$

para algún $D = p_1 \cdots p_{2r}, (D, N) = 1$?

Endomorfismos

Conjetura (R. Coleman). Hay un número finito de $\mathbb{Z}$-anillos R para los que existe A/K, $\dim(A) = g$, tal que

$$\mathrm{End}_K(A) \simeq R.$$

- Es cierta para $g = 1$.

Conjetura de Coleman para superfícies abelianas sobre $\mathbb{Q}$

1. Casos en que $A \overset{\bar{\mathbb{Q}}}{\sim} E_1 \times E_2$.

• $A = E_1 \times E_2$, E_1, E_2 curvas elípticas sobre $\mathbb{Q}$:

$$\mathrm{End}_{\mathbb{Q}}(A) = \begin{cases} \mathbb{Z} \times \mathbb{Z} & \text{si } E_1 \not\sim E_2 \text{ sobre } \mathbb{Q} \\ \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) : N \mid c \} & \text{si } 0 \to \mathbb{Z}/N\mathbb{Z} \to E_1 \to E_2 \to 0 \end{cases}$$

Teorema (B. Mazur). Existe un número finito de grados N de isogenias cíclicas entre curvas elípticas E_1, E_2 sobre $\mathbb{Q}$.

• Sea E/K, $[K:\mathbb{Q}]=2$, una $\mathbb{Q}$-curva elíptica sin CM de grado N: $\exists\,\varphi/K : E \sim E^{\sigma}$, $\mathrm{Ker}(\varphi)=\mathbb{Z}/N\mathbb{Z}$.

$A=\mathrm{Res}_{K/\mathbb{Q}}(E)$ es una superfície abeliana sobre $\mathbb{Q}$: $A \overset{K}{\sim} E\times E^{\sigma}$ y

$$\mathrm{End}^0_{\mathbb{Q}}(A)\simeq\mathbb{Q}(\sqrt{\pm N})$$

Conjetura (N. Elkies). Existe un número finito de grados N de $\mathbb{Q}$-curvas elípticas cuadráticas sin CM.

2. El caso en que A es absolutamente irreducible.

Teorema (G. Shimura, E. Pyle). Sea $A/\mathbb{Q}$, $\dim(A) = 2$, absolutamente irreducible. Entonces

$$\mathrm{End}^0_{\mathbb{Q}}(A) \simeq \begin{cases} \mathbb{Q} \\ \mathbb{Q}(\sqrt{m}), m > 1 \end{cases}$$

y

$$\mathrm{End}^0_{\mathbb{Q}}(A) \simeq \begin{cases} \mathbb{Q} & \text{(Espacio de móduli de dimensión 3)} \\ \mathbb{Q}(\sqrt{m}), m > 1 & \text{(dim 2)} \\ B_D, D = p_1 \cdots p_{2r}, r \geq 1 & \text{(dim 1)} \\ K/\mathbb{Q}, [K : \mathbb{Q}] = 4 & \text{(dim 0)} \end{cases}$$

Teorema (N. Murabayashi, A. Umegaki) Hay un número finito de cuerpos K, $[K:\mathbb{Q}]=4$, tales que existe $A/\mathbb{Q}$, $\dim(A)=2$, $\mathrm{End}^0_{\overline{\mathbb{Q}}}(A)\simeq K$.

Conjetura.

• Hay un número finito de enteros $m>1$, $\square \nmid m$, tales que existe $A/\mathbb{Q}$, $\dim(A)=2$:

$$\mathrm{End}^0_{\mathbb{Q}}(A)\simeq \mathbb{Q}(\sqrt{m}).$$

• Hay un número finito de (D,m), $\square \nmid m$, $D=p_1\cdots p_{2r}$, tales que existe $A/\mathbb{Q}$, $\dim(A)=2$:

$$\mathrm{End}^0_{\mathbb{Q}}(A)\simeq \mathbb{Q}(\sqrt{m}),\quad \mathrm{End}^0_{\overline{\mathbb{Q}}}(A)\simeq B_D$$

Decimos que (D,m) es un par *premodular* y que A lo realiza.

Interpretación modular

$X_D/\mathbb{Q}$ curva de Shimura de discriminante $D = p_1 \cdots p_{2r}$, $N = 1$.
Teorema (G. Shimura). X_D es el espacio de móduli grueso de superfícies abelianas polarizadas con multiplicación cuaterniónica por B_D.

$$X_D(\bar{\mathbb{Q}}) \qquad \leftrightarrows \qquad \{\, (A, \iota : B_D \hookrightarrow \mathrm{End}^0(A), \mathcal{L}) \,\}/\simeq_{\bar{\mathbb{Q}}}$$

Teorema (G. Shimura). Si $K \hookrightarrow \mathbb{R}$, $X_D(K) = \emptyset$.
No existe A/K, $\mathrm{End}^0_K(A) \simeq B_D$ si $K \hookrightarrow \mathbb{R}$.

$W_D := \{\omega_m : m \mid D\} = \langle \omega_{p_1}, ..., \omega_{p_{2r}} \rangle \simeq (\mathbb{Z}/2\mathbb{Z})^{2r}, \quad W_D \subseteq \mathrm{Aut}_{\mathbb{Q}}(X_D)$.

Conjetura. Para todo D, $W_D \simeq \mathrm{Aut}_{\mathbb{Q}}(X_D)$.

Teorema (V. Rotger).

- Si $D = 2p, 3p$, $W_D \simeq \mathrm{Aut}_{\mathbb{Q}}(X_D)$.

- Si $\exists\, p, q \mid D$, $p \equiv 1 \bmod 4$, $q \equiv 1 \bmod 3$, $W_D \simeq \mathrm{Aut}_{\mathbb{Q}}(X_D)$.

$S_m/\mathbb{Q}$ superfície de Hilbert que clasifica superfícies abelianas A polarizadas con $\mathbb{Q}(\sqrt{m}) \hookrightarrow \mathrm{End}^0(A)$.

Teorema (V. Rotger) Dado $\mathbb{Q}(\sqrt{m}) \hookrightarrow B_D$, la imagen de la curva X_D por el morfismo de olvido

$$\begin{array}{ccccc} \pi & X_D & \longrightarrow & S_m \\ & (A, \iota, \mathcal{L}) & \mapsto & (A, \iota_{|\mathbb{Q}(\sqrt{m})}, \mathcal{L}) \end{array}$$

es

$$\pi(X_D) = \begin{cases} X_D & \text{si } m \nmid D \\ X_D/\langle \omega_m \rangle & \text{si } m \mid D. \end{cases}$$

Si $A/\mathbb{Q}$ realiza un par (D, m), produce un punto racional $P \in \pi(X_D)(\mathbb{Q}) \subseteq S_m(\mathbb{Q})$.

Teorema (N. Bruin, V. Flynn, J. González, V. Rotger)
Un par (D, m) es premodular si y solo si $m \mid D$ y

$$\{ \quad P \in X_D/\langle \omega_m \rangle(\mathbb{Q}) :$$

$$\bullet\, \pi^{-1}(P) \subset X_D(\mathbb{Q}(\sqrt{-\delta})), \quad B_D \simeq \left(\frac{-\delta, m}{\mathbb{Q}}\right)$$

$$\bullet\, P \text{ no es un punto CM } \} \neq \emptyset$$

Teorema.

- **(V. Rotger)** Si $D > 546$, $X_D/\langle\omega_m\rangle(\mathbb{Q})$ es finito.
- **(V. Rotger, A. Skorobogatov, A. Yafaev)**
  - Si $m \neq D$ o $m \neq D/p$, $\quad X_D/\langle\omega_m\rangle(\mathbb{Q}) = \emptyset$.
  - Si $D = pq$, $m = q$ son dos primos impares tales que:

($q_{\overline{p)=1}}$ o $p \equiv 1 \bmod 12$ o $p \equiv q \equiv 1 \bmod 4$, $\quad X_D\langle\omega_m\rangle(\mathbb{Q}) = \emptyset$.

- Si $m = D$, $\quad X_D/\langle\omega_m\rangle(\mathbb{Q}_p) \neq \emptyset \quad \forall p \leq \infty$.

Conjetura. Existen infinitos valores de D y m: $X_D/\langle\omega_m\rangle(\mathbb{Q}) = \emptyset$ y viola el principio de Hasse sobre $\mathbb{Q}$.

Ejemplo. $X_{23\cdot 107}/\langle\omega_{107}\rangle$ viola el principio de Hasse sobre $\mathbb{Q}$.

Teorema (N. Bruin, V. Flynn, J. González, V. Rotger)

- Si (D, m) es un par premodular, entonces $m = D$ ó $m = \frac{D}{p}$, con $p \mid D$ no split en $\mathbb{Q}(\sqrt{D/p})$.

- Sea $D = pq$, p, q primos impares. Si $(\frac{q}{p}) = 1$ o $p \equiv 1 \bmod 12$ o $p \equiv q \equiv 1 \bmod 4$, $\quad (D, q)$ no es un par premodular.

- Sea $D > 546$. Existe un número finito de superfícies abelianas $A/\mathbb{Q}$ que realizan (D, m).

Ejemplo: $(10, 2)$ no es premodular sobre $\mathbb{Q}$.

- $X_{10} : x^2 + y^2 + 2 = 0, \quad g = 0, \quad X_{10} \not\simeq \mathbb{P}^1_{\mathbb{Q}}$.
- $X_{10}/\langle\omega_2\rangle : x^2 + y + 2 = 0, \quad X_{10}/\langle\omega_2\rangle \simeq \mathbb{P}^1_{\mathbb{Q}}$.
- Las dos antiimágenes de

$$P = (a, -2 - a^2) \in X_{10}/\langle\omega_2\rangle$$

son $(a, \pm\sqrt{-2 - a^2}) \in X_D(\bar{\mathbb{Q}})$.

Pero

$$B_{10} \not\simeq \left(\frac{-2 - a^2,\ 2}{\mathbb{Q}}\right)$$

Ejemplo.: $(91, 91)$ no es premodular sobre $\mathbb{Q}$.

- $X_{91}, \quad g = 7$, no conocemos ecuación.
- $X_{91}/\langle \omega_{91} \rangle : y^2 = -x^6 + 19x^4 - 3x^2 + 1, \quad g = 2.$
- $X_{91}/\langle \omega_{91} \rangle(\mathbb{Q}) = \{(0, \pm 1), (\pm 1, \pm 4), (\pm 3, \pm 28)\}.$

Los 10 puntos son CM.