Cálculo de puntos ATR de Darmon en curvas elípticas no geométricamente modulares

Xevi Guitart[1] Marc Masdeu[2]

[1]Universitat Politècnica de Catalunya and Max Planck Institute for Mathematics

[2]Columbia University

ICMAT 2012, Madrid

Índex

Puntos racionales en curvas elípticas

- E una curva elíptica definida sobre $\mathbb{Q}$:

  $$E\colon y^2 + b_1xy + b_3y = x^3 + b_2x^2 + b_4x + b_6, \quad b_i \in \mathbb{Z}, \quad N = \mathrm{cond}(E)$$

- $E(\mathbb{Q}) = \{(x, y) \in E\colon x, y \in \mathbb{Q}\} \cup \{\infty\}$ tiene estructura de grupo abeliano.

Teorema de Mordell–Weil

$E(\mathbb{Q})$ es finitamente generado: $E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus E_{\mathrm{tors}}$

r: rango de $E/\mathbb{Q}$
E_{tors}: subgrupo de torsión.

- E_{tors} está perfectamente entendido:
  - Mazur: $\#E_{\mathrm{tors}} \leq 16$.
  - Nagell–Lutz: dada E se puede calcular fácilmente E_{tors}.
- Sobre r sabemos mucho menos.
  - Se conjetura que verifica una especie de principio “local-global”.
  - Entra en juego $L(E/\mathbb{Q}, s)$.

Función L y conjetura de Birch y Swinnerton–Dyer

- Para cada primo $p \in \mathbb{Z}$ definimos $a_p := p + 1 - \#E(\mathbb{Z}/p\mathbb{Z})$

Función L

$$L(E/\mathbb{Q}, s) = \prod_{p \nmid N} \frac{1}{(1 - a_p p^{-s} + p^{1-2s})} \prod_{p|N} \frac{1}{(1 - a_p p^{-s})} = \sum_{n \geq 1} a_n n^{-s}$$

- Esta expresión converge para $\Re(s) > 3/2$, pero gracias al teorema de modularidad admite una continuación analítica a $\mathbb{C}$.

Conjetura de Birch y Swinnerton-Dyer (BSD)

rango$(E(\mathbb{Q})) = \operatorname{ord}_{s=1} L(E/\mathbb{Q}, s)$.

Teorema (Gross–Zagier, Kolyvagin)

BSD es cierta si $\operatorname{ord}_{s=1} L(E/\mathbb{Q}, s) \leq 1$.

- Si $\operatorname{ord}_{s=1} L(E/\mathbb{Q}, s) = 1$ entonces se puede calcular un punto de orden infinito con el método de puntos de Heegner

Puntos de Heegner

Teorema de modularidad (Wiles *et al.*, 2001)

Existe una forma modular $f_E \in S_2(\Gamma_0(N))$ tal que $L(E/\mathbb{Q}, s) = L(f_E, s)$

- $f_E(z) = \sum_{n\geq 1} a_n e^{2\pi i n z}, \qquad a_p = p + 1 - \#E(\mathbb{F}_p)$
- $\omega_{f_E} = (2\pi i) f_E(z) dz$ define una diferencial holomorfa en $X_0(N)$
  - $X_0(N)/\mathbb{Q}$ curva modular de nivel N, $X_0(N)(\mathbb{C}) \simeq \Gamma_0(N) \setminus \mathcal{H}^*$
- $K \subset \mathbb{C}$ cuadrático imaginario, $\tau \in K \cap \mathcal{H}$

$$J_\tau = \int_{i\infty}^{\tau} \omega_{f_E} \in \mathbb{C}/\Lambda_{f_E} \sim E(\mathbb{C})$$

$\Lambda_{f_E} = \{\int_\gamma \omega_{f_E} \mid \gamma \in H_1(X_0(N), \mathbb{Z})\}$

- $J_\tau \in E(H_\tau)$, H_τ/K finita abeliana
- $P_K = \mathrm{Tr}_K^{H_\tau}(J_\tau) \in E(K)$ orden infinito $\iff \mathrm{ord}_{s=1} L(E/K, s) = 1$
- Propiedad clave: E es geometricamente modular

$$\pi_E \colon X_0(N) \longrightarrow E$$

$\tau \in X_0(N)(H_\tau)$ y $J_\tau = \pi_E(\tau)$

Curvas sobre cuerpos totalmente reales

- E/F, con F cuerpo totalmente real, $\mathrm{cond}(E) = \mathcal{N} \subset F$
  - $E(F)$ grupo abeliano finitamente generado
  - E/F también es modular: f_E es una forma modular de Hilbert
  - Conjetura BSD: $\mathrm{rank}(E(F)) = \mathrm{ord}_{s=1} L(E/F, s)$

Teorema (Gross–Zagier, Kolyvagin, Zhang)

Supongamos que E satisface la siguiente condición:

(JL) $[F\colon \mathbb{Q}]$ es impar o existe $\mathfrak{p}$ tal que $\mathrm{ord}_{\mathfrak{p}}(\mathcal{N})$ impar.

entonces *BSD* se cumple si $\mathrm{ord}_{s=1} L(E/F, s) \leq 1$.

- Si E verifica (JL) entonces es geometricamente modular:

  $$\pi_E\colon \mathrm{Jac}(X) \to E, \quad X/F \text{ curva de Shimura}$$

  Hay puntos de Heegner si E es geometricamente modular.
- Si E no verifica (JL): no es geometricamente modular en general.
  - Si E es $\mathbb{Q}$-curva (i.e., si $E^\sigma \sim E$ para todo $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$): entonces sí es geometricamente modular
- Si E no verifica (JL) y no es $\mathbb{Q}$-curva, no se conoce ningún método sistemático para calcular puntos de orden infinito.

Método de los puntos ATR (caso más sencillo)

- F cuerpo cuadrático real y E/F una curva elíptica de conductor 1
  e.g, para fijar ideas: $F = \mathbb{Q}(\sqrt{509})$, $\omega = \frac{1+\sqrt{509}}{2}$, $h^+(F) = 1$

  $$E_{509}\colon y^2 - xy - \omega y = x^3 + (2+2\omega)x^2 + (162+3\omega)x + (71+34\omega)$$

- Sean $v_0, v_1 : F \hookrightarrow \mathbb{R}$ y consideremos K/F ext. cuadrática ATR
  - v_0 extiende a una plaza compleja de K
  - v_1 extiende a un par de plazas reales de K
- Objetivo: "producir" $P_K \in E(K)$ como una integral de ω_{f_E}
- La forma modular de Hilbert asociada a E es $f_E\colon \mathcal{H}\times\mathcal{H} \longrightarrow \mathbb{C}$

  $$f_E(z_0, z_1) := \sum_{n\in\mathcal{O}_F^+} a_n e^{2\pi i(v_0(n/d)z_0 + v_1(n/d)z_1)}$$

  $a_n \in \mathbb{Z} \rightsquigarrow$ contando puntos en $E \mod \mathfrak{p}$, para $\mathfrak{p} \subseteq F$
- $\omega_{f_E} = (2\pi i)^2 f_E(z_0, z_1) dz_0 dz_1$ forma diferencial de $\mathcal{H}\times\mathcal{H}/\mathrm{SL}_2(\mathcal{O}_F)$
- $X := (\mathcal{H}\times\mathcal{H})/\mathrm{SL}_2(\mathcal{O}_F)$ es la superfície modular de Hilbert

Definición de los puntos ATR

- $\varphi\colon K \hookrightarrow \mathrm{M}_2(F)$ un embedding optimal (i.e., $\varphi(\mathcal{O}_K) \subseteq \mathrm{M}_2(\mathcal{O}_F)$)
  - $\varphi(K^\times)$ tiene un único punto fijo $\tau_0 \in \mathcal{H}$, actuando via v_0
  - $\varphi(K^\times)$ tiene dos puntos fijos $\tau_1, \tau_1' \in \mathbb{R} = \partial\mathcal{H}$, actuando via v_1
- $\{\tau_0\} \times \{\tau_1 \to \tau_1'\} \subset \mathcal{H} \times \mathcal{H}$
- Sea R_φ su imagen en $X = \mathcal{H} \times \mathcal{H}/\mathrm{SL}_2(\mathcal{O}_F)$
- $R_\varphi \in H_1(X, \mathbb{Z})$ y existe $T_\varphi \in C_2(X, \mathbb{Z})$ tal que $\partial T_\varphi = R_\varphi$
- Punto ATR asociado a φ: para una cierta diferencial ω_f^+

$$J_\varphi = \int_{T_\varphi} \omega_{f_E}^+ \in \mathbb{C}/\Lambda_{f_E} \sim E \quad \text{(Conjetura de Oda)}$$

Conjetura (Darmon)

- $J_\varphi \in E(H)$, donde H es el cuerpo de clases de Hilbert de K.
- $P_K = \sum_\varphi J_\varphi \in E(K)$ orden infinito si y sólo si $\mathrm{ord}_{s=1} L(E/K, s) = 1$.

- Darmon–Logan: algoritmo para calcular T_φ explícitamente
  - La conjetura se puede testear numéricamente.

Evidencia numérica

- El algoritmo de Darmon–Logan tenía algunas restricciones computacionales.
- Testearon la conjetura para tres curvas elípticas E_{29}, E_{37}, E_{41}:
  - son $\mathbb{Q}$-curvas, y por tanto geométicamente modulares
  - los puntos ATR, en este caso particular, son múltiplos de los puntos de Heegner (Darmon–Rotger–Zhao).

Objetivo

Calcular un punto ATR en una curva que no sea $\mathbb{Q}$-curva, y dar la primera evidencia numérica de que el método funciona para curvas que no son geometricamente modulares.

- La "primera" curva elíptica de conductor 1 sobre un cuadrático real que no es $\mathbb{Q}$-curva es E_{509}.
- Para calcular el punto ATR, primero tuvimos que eliminar las restricciones computacionales del algoritmo de Darmon y Logan.

Punto ATR en la curva E_{509}

- $F = \mathbb{Q}(\sqrt{509})$, $\omega = \frac{1+\sqrt{509}}{2}$

  $E_{509}\colon y^2 - xy - \omega y = x^3 + (2+2\omega)x^2 + (162+3\omega)x + (71+34\omega)$

- $K = F(\sqrt{\alpha})$, $\alpha = 9144\omega + 98577$, $[H\colon K] = 2$.
- $(\omega + 17, \frac{\sqrt{\alpha}+\sqrt{509}+18}{2}) \in E(K)$ punto de orden infinito $\leftrightarrow z \in \mathbb{C}/\Lambda_E$
- DL "mejorado": hemos calculado $J_K = J_{\varphi_1} + J_{\varphi_2}$ hasta 12 dígitos
  - $a_{\mathfrak{n}}$ para $|\mathfrak{n}| \leq 4 \cdot 10^8$
  - Tiempo de cálculo: unos 2 días en una máquina con 32 procesadores y 320 GB (cálculos paralelizables)
- $J_K \simeq -4z$ (hasta 12 dígitos)
- Esto nos da una verificación numérica de que el punto ATR es de orden infinito, tal y como predice la conjetura de Darmon.

Fracciones contínuas en F

- Un paso del algoritmo de Darmon–Logan consiste en calcular la fracción contínua de un elemento $c \in F$:

$$c = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdots + \frac{1}{q_n}}}, \quad q_1, \ldots, q_n \in \mathcal{O}_F$$

- Si F es euclideo los q_i se calculan con el algoritmo de euclides
- Hay un número finito de $\mathbb{Q}(\sqrt{d})$ euclideos ($\mathbb{Q}(\sqrt{73})$ es el último)
- Conjecturalmente todos los $\mathbb{Q}(\sqrt{d})$ con número de clases 1 son euclideos en 2 pasos: para todo $a, b \in \mathcal{O}_F$ existen q_1, q_2, r_1, r_2

$$a = bq_1 + r_1;\ b = q_2 r_1 + r_2;\ \mathrm{Nm}_{F/\mathbb{Q}}(r_2) < \mathrm{Nm}_{F/\mathbb{Q}}(b)$$

- Cooke: método para verificar si $\mathbb{Q}(\sqrt{d})$ es E_2 (e.g. $\mathbb{Q}(253)$)
- Adaptación algorítmica del método

Teorema (G.-Masdeu)

Todos los $\mathbb{Q}(\sqrt{d})$ con número de clases 1 y $d \leq 8000$ son E_2.

Integrales de formas modulares de Hilbert

- $\int_x^y \int_z^t \omega_f = \int_x^y \int_z^t \sum_n a_n e^{2\pi i(n_0 z_0/d_0 + n_1 z_1/d_1)}$
- Para que converja rápidamente necesitamos que $\Im(x), \Im(y), \Im(z), \Im(t) >> 0$
- Esto determina el número de coeficientes de Fourier a_n necesarios.
- Problema: no controlamos muy bien las partes imaginarias de las integrales que produce el algoritmo de Darmon–Logan
- Idea: utilizar que los limites son invariantes por $\mathrm{SL}_2(\mathcal{O}_F)$

Teorema (G.-Masdeu)

Existe una constante ϵ_F, que depende sólo de F, tal que toda integral se puede escribir como

$$\int_x^y \int_z^t \omega_f = \int_{x_1}^{y_1} \int_{z_1}^{t_1} \omega_f + \cdots + \int_{x_n}^{y_n} \int_{z_n}^{t_n} \omega_f$$

con $\Im(x_1), \Im(y_i), \Im(z_i), \Im(t_i) \geq \epsilon_F$.

Otra aplicación (futura) del algoritmo de puntos ATR

- Los puntos ATR son la base de un algoritmo de L. Dembélé para calcular curvas elípticas E/F con buena reducción en todos los primos, a partir de la forma modular de Hilbert.
- Hasta el momento hay tablas con algunas de estas ecuaciones
  - se calculan haciendo cribas en ecuacioes de curvas
  - no son completas, ni sistemáticas
- El algoritmo de Dembélé, junto con el algoritmo de puntos ATR proporcionan un método sistemático para calcularlas, y producir tablas concretas (digamos hasta $\mathbb{Q}(\sqrt{d})$ con $d \leq 2000$).
- Esperamos poder utilizar el método de Dembélé, junto con nuestro algoritmo, para calcular estas ecuaciones.

Cálculo de puntos ATR de Darmon en curvas elípticas no geométricamente modulares

Xevi Guitart[1] Marc Masdeu[2]

[1]Universitat Politècnica de Catalunya and Max Planck Institute for Mathematics

[2]Columbia University

ICMAT 2012, Madrid