La conjetura *abc* y la conjetura de Szpiro

Ignacio Henríquez, con apuntes y un apéndice de José Cuevas Barrientos

Resumen. En esta charla estudiaremos la relación entre la conjetura *abc* y la conjetura de Szpiro y veremos que son «casi equivalentes». Más precisamente, mostraremos que la conjetura *abc* implica la conjetura de Szpiro y que ésta última implica una versión un poco más débil de la primera.

1. La conjetura de Szpiro

Recuérdese que una curva elíptica E sobre un cuerpo k con $\operatorname{car} k \nmid 6$ siempre es isomorfa a una dada por una ecuación de Weierstrass corta

$$E\colon \quad y^2 = x^3 - 27c_4x - 54c_6, \qquad c_4, c_6 \in k, \tag{1}$$

la cual posee un discriminante Δ que satisface que $1728\Delta = c_4^2 - c_6^2$. Si k es un cuerpo numérico (i.e., una extensión finita de $\mathbb{Q}$), entonces podemos elegir una ecuación 1 para E donde $c_4, c_6 \in \mathcal{O}_k$ sean enteros algebraicos. En éste caso, existe una noción de *discriminante minimal* (cfr. Silverman [**5,** pág. 243]) el cual es, en general, un ideal en $\mathcal{O}_k$, pero cuando $k = \mathbb{Q}$ podemos definirlo de la siguiente manera con un número:

Definición 1.1: Sea E una curva elíptica sobre $\mathbb{Q}$. Su ***discriminante minimal*** $D_{E/\mathbb{Q}}$ (también denotado como $\Delta_E^{\min}$) es el discriminante Δ de una ecuación de Weierstrass (1) con $c_4, c_6 \in \mathbb{Z}$ tal que dada otra ecuación de Weierstrass con coeficientes en $\mathbb{Z}$ y con discriminante Δ' se satisfaga que $|\Delta| \leq |\Delta'|$. En cuyo caso, la ecuación (1) se dice ***minimal***.

Proposición 1.2: Sea E una curva elíptica sobre $\mathbb{Q}$ dada por una ecuación de Weierstrass (1) con $c_4, c_6 \in \mathbb{Z}$ y con discriminante Δ. Existen $u, r, s, t \in \mathbb{Z}$ tales que el cambio de variables

$$x = u^2x' + r, \qquad y = u^3y' + u^2sx' + t \tag{2}$$

induce la ecuación minimal $y'^2 = x'^3 - 27c_4'x' - 54c_6'$ con

$$u^4c_4' = c_4, \qquad u^6c_6' = c_6, \qquad u^{12}D_{E/\mathbb{Q}} = \Delta.$$

Demostración: El que sobre $\mathbb{Q}$ siempre exista el discriminante minimal es el Cor. VIII.8.3 de Silverman [**5,** pág. 245]. Los *cambios de variables*

Fecha: 10 de mayo de 2024.

admisibles sobre una ecuación de Weierstrass vienen detallados en KNAPP [**2,** pág. 63]. □

Recuérdese la siguiente noción:

Definición 1.3: El ***conductor*** de una curva elíptica E sobre $\mathbb{Q}$:

$$N_{E/\mathbb{Q}} := \prod_p p^{f_p(E)},$$

donde

$$f_p(E) := \begin{cases} 0, & E \text{ tiene buena reducción en } p, \\ 1, & E \text{ tiene reducción multiplicativa en } p, \\ 2, & E \text{ tiene reducción aditiva en } p, \end{cases}$$

para todo primo $p \nmid 6$.

Observación 1.3.1: Para los primos $p \in \{2, 3\}$ la definición es más complicada, pero existe la cota uniforme $0 \leq f_p(E) \leq 8$. (Para más detalles, vid. §A.2 más adelante.)

Ahora, recuérdese la siguiente conjetura de la charla anterior:

Conjetura de Szpiro (1983) 1.4: Para todo $\epsilon > 0$, existe una constante $\kappa_\epsilon > 0$ con la siguiente propiedad: para toda curva elíptica E sobre $\mathbb{Q}$ se satisface la siguiente desigualdad

$$|D_{E/\mathbb{Q}}| \leq \kappa_\epsilon \cdot N_{E/\mathbb{Q}}^{6+\epsilon}.$$

Al igual que con la conjetura *abc*, algún caso particular de la conjetura de Szpiro para un $\epsilon > 0$ fijo se denomina «conjetura de Szpiro *débil*».

Teorema 1.5: Se cumplen:

1. La conjetura de Szpiro implica la conjetura *abc* débil con exponente $3/2 + \epsilon$ (para todo $\epsilon > 0$).
2. La conjetura *abc* implica la conjetura de Szpiro.

DEMOSTRACIÓN: $1 \implies 2$. Sea $0 < a < b$ enteros coprimos y sea $c := a + b$ el cual satisface que $b < c < 2b$. Considere la clausura proyectiva de la curva E sobre $\mathbb{Q}$ dada por la ecuación de Weierstrass

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

el cual tiene discriminante $\Delta = 16(abc)^2$, de modo que E es una curva elíptica. Además, su ecuación de Weierstrass (inducido por los cambios de variables descritos en [**5,** pág. 42]) tiene

$$\begin{aligned} c_4 &= 16(a^2 + ab + b^2) = 16(c^2 - ab), \\ c_6 &= -32(2a^3 + 3a^2b + 3ab^2 + 2b^3) = -32(c^3 + a^3 + b^3). \end{aligned}$$

Por la proposición anterior sean $u, r, s, t \in \mathbb{Z}$ tales que el cambio de variables (2) induce la ecuación minimal; entonces

$$u^4 \mid c_4, \qquad u^6 \mid c_6.$$

Así pues, nos preguntamos por divisores comunes de c_4 y c_6. Podemos notar que

$$c^3 + a^3 + b^3 - a(c^2 - ab) = c^3 + a(a^2 + ab - c^2) + b^3 = c^3 + abc + b^3$$

y simétricamente

$$c^3 + a^3 + b^3 - b(c^2 - ab) = c^3 + a^3 + abc,$$
$$c^3 + a^3 + b^3 - c(c^2 - ab) = abc + a^3 + b^3.$$

Así pues, si $p \neq 2$ es un primo tal que $p \mid \mathrm{mcd}\{c_4, c_6\}$ vemos que

$$p \mid \mathrm{mcd}\{a^3 - b^3, a^3 - c^3, b^3 - c^3\} = \mathrm{mcd}\{2a^3, 1b^3, 2c^3\} = 2.$$

Por lo que u es una potencia de 2 y, a mano, podemos ver que de hecho $u \in \{1, 2\}$, de modo que

$$D_{E/\mathbb{Q}} = 16(abc)^2 \qquad \text{o} \qquad D_{E/\mathbb{Q}} = 2^{-8}(abc)^2.$$

En cualquier caso, $|D_{E/\mathbb{Q}}| \geq 2^{-8}(abc)^2$, así que obtenemos que

$$2^{-8}(abc)^2 \leq |D_{E/\mathbb{Q}}| \leq \kappa_\epsilon \cdot (6^8)^{6+\epsilon} \prod_{p \mid abc} p^{6+\epsilon},$$

donde empleamos los siguientes datos: que las potencias de 2 y 3 que aparecen en $N_{E/\mathbb{Q}}$ son ≤ 8 (obs. 1.3.1), y que si p es un primo impar que divide a Δ (equivalentemente, $p \mid abc$), entonces $p \nmid c_4$, por lo que E tiene reducción multiplicativa en p.

Finalmente, empleando que $1 \leq a$ y $b \geq \frac{1}{2}c$ obtenemos que

$$c^4 \leq \underbrace{\kappa_\epsilon 2^{10} \cdot (6^8)^{6+\epsilon}}_{\mu_\epsilon} \mathrm{Rad}(abc)^{6+\epsilon};$$

donde μ_ϵ es una constante que solo depende de ϵ. Tomando raíces cuartas obtenemos la conjetura *abc* débil con exponente $3/2 + \epsilon$.

$2 \implies 1$. Sea $E/\mathbb{Q}$ una curva elíptica dada por una ecuación de Weierstrass minimal (1) y supongamos que c_4 y c_6 son coprimos. Gracias a la identidad $1728\Delta = c_4^3 - c_6^2$ podemos aplicar la conjetura *abc* con

$$a := c_4^3, \qquad b := -c_6^2, \qquad c := 1728\Delta,$$

lo que da

$$\mathrm{máx}\{|c_4|^3, c_6^2, |1728\Delta|\} \leq \kappa_\epsilon \cdot \prod_{p \mid 6c_4c_6\Delta} p^{1+\epsilon}.$$

La coprimalidad de c_4 y c_6 implica que E tiene pura reducción multiplicativa, por lo que podemos acotar

$$\kappa_\epsilon \cdot \prod_{p \mid 6c_4c_6\Delta} p^{1+\epsilon} \leq \mu_\epsilon |c_4c_6N_{E/\mathbb{Q}}|^{1+\epsilon}.$$

donde $\mu_\epsilon := \kappa_\epsilon 6^{-6-6\epsilon}$; esto da

$$|c_4|^{2-\epsilon} \leq \mu_\epsilon |c_6 N_{E/\mathbb{Q}}|^{1+\epsilon},$$

la cual elevamos a la potencia $2+2\epsilon$

$$|c_6|^{1-\epsilon} \leq \mu_\epsilon |c_4 N_{E/\mathbb{Q}}|^{1+\epsilon},$$

la cual elevamos a la potencia $3+3\epsilon$ y

$$|1728\Delta| \leq \mu_\epsilon |c_4 c_6 N_{E/\mathbb{Q}}|^{1+\epsilon},$$

la cual elevamos a la potencia $1-5\epsilon$. Multiplicando todo y despejando, se obtiene

$$|\Delta|^{1-5\epsilon} \leq \mu_\epsilon^6 N_{E/\mathbb{Q}}^{6+6\epsilon} \implies |\Delta| \leq \mu_\epsilon N_{E/\mathbb{Q}}^{6+\frac{36\epsilon}{1-5\epsilon}}.$$

Finalmente, basta ajustar los exponentes para recuperar la conjetura de Szpiro. □

Observación 1.5.1: Más precisamente, es fácil observar que la prueba indica que la conjetura de Szpiro débil implica una versión débil de la conjetura *abc*, y viceversa.

Apéndice A. Comentarios adicionales

A.1. Una generalización de la conjetura de Szpiro. Similar a la demostración del teorema 1.5, podemos probar lo siguiente:

Teorema A.1: Las siguientes conjeturas son equivalentes:

1. La conjetura *abc* (fuerte) de Masser-Oesterlé.
2. **La conjetura generalizada de Szpiro:** Para todo $\epsilon > 0$ existe una constante universal $\kappa_\epsilon > 0$ con la siguiente propiedad: Sea E una curva elíptica sobre $\mathbb{Q}$ con ecuación de Weierstrass minimal $y^2 = x^3 - 27c_4x - 54c_6$, entonces

$$\text{máx}\{|\Delta|, |c_4|^3\} \leq \kappa_\epsilon N_{E/\mathbb{Q}}^{6+\epsilon}.$$

Demostración: La demostración no es demasiado avanzada y está perfectamente al alcance del lector. Ésta está detallada en Bombieri y Gubler [**1,** págs. 431 s.]. □

A.2. Sobre el conductor. Ésta sección es un resumen de resultados detallados en Silverman [**4,** págs. 379 ss.], §IV.10.

Definición A.2: Sea E una curva elíptica sobre un cuerpo K y sea $n > 1$ un entero. Denotemos por L la mínima extensión normal de K que contiene a toda la n-torsión $E(K^{\text{alg}})[n]$; entonces existe una acción canónica (llamada ocasionalmente como la *representación de Galois n-ádica*)

$$\text{Gal}(L/K) \curvearrowright E[n],$$

y más generalmente, una acción sobre cualquier subgrupo $H \leq \mathrm{Gal}(L/K)$.

Sea K un cuerpo local ultramétrico con cuerpo de restos k de característica $p > 0$ y sea $n := \ell$ un primo distinto de p. Asociado a la extensión L/K tenemos los *grupos de ramificación* (vid. NEUKIRCH [**3,** págs. 176 s.], Def. II.10.1):

$$\mathrm{Gal}(L/K) = G_{-1}(L/K) \supseteq G_0(L/K) \supseteq G_1(L/K) \supseteq \cdots = \{\mathrm{Id}_L\}$$

los cuales tienen cardinalidad (finita) $g_i(L/K) := |G_i(L/K)|$. Definimos la ***parte salvaje del conductor*** de E/K como

$$\delta(E/K) := \sum_{j=1}^{\infty} \frac{g_j(L/K)}{g_0(L/K)} \dim_{\mathbb{F}_\ell}\big(E[\ell]/E[\ell]^{G_i(L/K)}\big),$$

donde el superíndice «$G_i(L/K)$» denota el subconjunto fijo por la acción. Definimos la ***parte moderada del conductor*** de E/K como

$$\varepsilon(E/K) := \begin{cases} 0, & E \text{ tiene buena reducción en } k, \\ 1, & E \text{ tiene reducción multiplicativa en } k, \\ 2, & E \text{ tiene reducción aditiva en } k. \end{cases}$$

Y definimos el ***exponente del conductor*** como

$$f(E/K) := \varepsilon(E/K) + \delta(E/K).$$

Observación A.2.1: Nótese que como $G_j(L/K) = \{1\}$ para $j \gg 0$, concluímos que la sumatoria es finita.

Como se puede apreciar, la parte salvaje es precisamente lo que nos interesa cuando $p \in \{2, 3\}$:

Teorema A.3: Sea E una curva elíptica sobre un cuerpo local K ultramétrico con cuerpo de restos de característica $p > 0$.

1. La definición de $\delta(E/K)$ no depende de la elección del primo $\ell \neq p$.
2. Cuando $p \geq 5$ se cumple que $\delta(E/K) = 0$.

DEMOSTRACIÓN: Cfr. [**4,** pág. 381], Thm. IV.10.2. □

También hay una definición, en términos de la representación de Galois ℓ-ádica de $\varepsilon(E/K)$, pero uno prueba que coincide con la aquí presentada (véase el mismo teorema descrito arriba).

Aún así, la parte salvaje del conductor tiene una cota cuando $p \mid 6$:

Teorema A.4 (Brumer-Kramer-Lockhart-Rosen-Silverman): Sea $K/\mathbb{Q}_p$ un cuerpo local con valuación normalizada v_K. Para toda curva elíptica E sobre K, el exponente del conductor está acotado por

$$f(E/K) \leq 2 + 3v_K(3) + 6v_K(2).$$

DEMOSTRACIÓN: Cfr. [**4,** págs. 385 ss.], Thm. IV.10.4. □

Observación A.4.1: En la situación *global* de $K = \mathbb{Q}$ esto implica las cotas eficientes de $f_2(E) \leq 8$ y $f_3(E) \leq 5$.

Finalmente, hay otra manera más geométrica de calcular el exponente del conductor sin pasar por representaciones:

Teorema A.5 (fórmula de Ogg): Sea $K/\mathbb{Q}_p$ un cuerpo local y E una curva elíptica sobre K. Entonces:

$$v_K(\mathfrak{D}_{E/K}) = f(E/K) + m(E/K) - 1,$$

donde $v_K(\mathfrak{D}_{E/K})$ es la valuación del discriminante minimal (local, vid. SILVERMAN [**5,** pág. 186]) y $m(E/K)$ es la cantidad de componentes irreducibles geométricas de la fibra especial de E/K.

DEMOSTRACIÓN: Cfr. [**4,** págs. 389 ss.], Thm. IV.11.1. □

El número $m(E/K)$ viene dado por el algoritmo de Tate.

REFERENCIAS

1. BOMBIERI, E. y GUBLER, W. *Heights in Diophantine Geometry* (Cambridge University Press, 2006).
2. KNAPP, A. W. *Elliptic Curves* (Princeton University Press, 1992).
3. NEUKIRCH, J. *Algebraic Number Theory* trad. por SCHAPPACHER, N. (Springer-Verlag Berlin Heidelberg, 1992).
4. SILVERMAN, J. H. *Advanced Topics in the Arithmetic of Elliptic Curves Graduate Texts in Mathematics* **151** (Springer-Verlag, 1994).
5. SILVERMAN, J. H. *The arithmetic of elliptic curves* 2.ª ed. (Springer-Verlag, 2009).

Correo electrónico: ignacio.henriquez@uc.cl

DEPARTAMENTO DE MATEMÁTICAS, PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE. FACULTAD DE MATEMÁTICAS, 4860 AV. VICUÑA MACKENNA, MACUL, RM, CHILE
Correo electrónico: josecuevasbtos@uc.cl