Cuando tuerces curvas elípticas sobre cuerpos numéricos

Edgar Delgado Vega

26 de mayo de 2025 | Compilado el 30 de abril de 2026, v.0.0.1

1. Ventanal rüido

Comencemos con escuchar un lepidóptero por la ventana e intentemos pintarlo en su vuelo estival:

$$y^2 = x^3 + ax + b \longmapsto \text{He aquí su cuerpo instantáneo.}$$

Tres o cuatro siglos después, su efluvio permanece en

$$E(K) = E(K)_{\text{tors}} \oplus \mathbb{Z}^{\mathcal{R}}.$$

Observación 1.1. Las demostraciones básicas se encuentran en uno de los libros por defecto para este tema: *De las elípticas, su curva, la aritmética* [Sil09] Título excesivamente encriptado y con el hipérbaton desbocado. (léase más abajo a Yoda).

Usualmente, cuando empezamos a sumar elementos que interpretamos como clases de equivalencias $\overline{p}$ en grupos cíclicos finitos $\mathbb{Z}/n\mathbb{Z} = C_n$, nos encontramos con que todo elemento, sumado consigo mismo el número adecuado de veces ("vuelve a la tierra en que nació", como pluraliza el vals de César Miró) hacia la identidad e del grupo C_n.

Nos corresponde en este compás, abstraer lo afín o proyectivo. Sabemos que la misma jugada temporal se da en curvas elípticas $E(\mathbb{Q})$, solo que aquí la composición se interpreta mediante un procedimiento geométrico de trazados de recta y tangente. Este fenómeno pictórico se llama torsión. Si un punto $P \in E(\mathbb{Q})$ cumple que, al sumarlo n veces, se llega a la identidad geométrica

$$P \oplus P \oplus \cdots \oplus P = \mathcal{O},$$

diremos que P es un punto de torsión de orden n, y el subgrupo cíclico que genera $\langle P \rangle$ es un subgrupo de torsión de orden n.

Para llevar a cabo el cómputo de este apunte, no importa probar que este conjunto es finito, pues efectivamente lo es. Saltemos.

2. Teorema de Mazur

En 1977, Barry Mazur demostró, en un artículo extenso [Maz77, Teorema 8], exactamente a qué conjunto de grupos cíclicos son isomorfos los puntos de

torsión $E(\mathbb{Q})_{\text{tors}}$. La lista se escinde en dos casos pequeños

$$T_1 = \{C_n \mid n = 1, 2, \ldots, 10, 12\}$$

y el producto de dos grupos cíclicos

$$T_2 = \{C_2 \times C_{2n}, \mid n = 1, 2, 3, 4\}.$$

Sí, es muy acuarélica cuestión, pues, a pesar de haber infinitas curvas elípticas sobre $\mathbb{Q}$, su estructura de torsión es así de corta (15 no es nada). Por ende,

$$E(\mathbb{Q})_{\text{tors}} \in T_1 \cup T_2. \tag{1}$$

Sí, en efecto, es van Gogh (¿se perdieron estas pinturas?).

3. Dimensión 2 sobre racionales

Llevemos la jugada una dimensioncita vectorial más alta, en otras palabras, $K = \mathbb{Q}(\sqrt{D})$, con D libre de cuadrados. Y planteamos la pregunta: ¿cómo es $E(K)_{\text{tors}}$, también es una lista breve?

3.1. Teorema de Kamienny, Kenku y Momose

En varios artículos a fines del siglo XX (búscalos en [GJLR17] o por la web, que aquí se corta el internet), Kenku y Momose, y finlandiamente Kamienny, probaron la lista en completitud como se aprecia en el siguiente cuadro de Ingres:

$$T_1 = \{C_n \mid n = 1, 2, \ldots, 16, 18\}$$

y los productos de grupos

$$T_2 = \{C_2 \times C_{2n} \mid n = 1, 2, \ldots, 6\},$$

$$T_3 = \{C_3 \times C_{3n} \mid n = 1, 2\},$$

$$T_4 = \{C_4 \times C_4\}.$$

Nos queda juntar las piezas del légamo, que diga, del grupocabezas, y nos aparece

$$E(K)_{\text{tors}} \in T_1 \cup T_2 \cup T_3 \cup T_4. \tag{2}$$

Observación 3.1. Recordemos que $T_2 = C_2 \times C_{2n}$ escapa a lo cíclico, porque $\gcd(2, 2n) = 2 \neq 1$. Ya que el vaho del amanecer se disipa: si n es impar, podemos descomponer T_2 en partículas más diminutas usando el teorema de descomposición de grupos abelianos finitos (uno de los teoremas muy bravos)

$$T_2 \cong C_2 \times C_2 \times C_n \cong V_4 \times C_n, \tag{3}$$

lo que nos recuerda que el grupo de Klein (*Vierergruppe*) también está por aquí, acompañado de un factor cíclico C_n.

4. A mayor dimensión, más chanfaina el grupo de torsión

Con lo visto en curvas elípticas sobre cuerpos cuadráticos y en general (a ver si un día vemos con caleidoscopio el teorema de Mordell-Weil grabado en aroma al inicio), los grupos posibles son, para cualquier cuerpo numérico K, tal como se esboza en blanco y negro a continuación:

$$E(K)_{\text{tors}} \in C_m \times C_n. \tag{4}$$

Además, ya lo viste en acción:

$$m|n.$$

¿Hay listas finitas para cuerpos cúbicos, bicuadráticos y más? Sí, pero no las veremos aquí por precaución. Como diría el Yoda extremo permutador, la completitud de las listas (los posibles m y n) es menester decir que probar nos es desconocido aún.

Observación 4.1. Las rimas vinieron de la nada.

Antes de terminar y que se pierda para siempre el efluvio primero, Merel [Mer96], en mil nueve noventa y seis (al estilo expositor de Ana Lucía Frega), probó que para cualquier $E(K)$, la torsión tiene orden acotado; de modo que $B([K:\mathbb{Q}])$ no escapa al infinito, así como la memoria de nuestro lepidóptero.

Referencias

[GJLR17] Enrique González-Jiménez and Álvaro Lozano-Robledo. On the torsion of rational elliptic curves over quartic fields. *Mathematics of Computation*, 87(311):1457–1478, August 2017.

[Maz77] Barry Mazur. Modular curves and the eisenstein ideal. *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, 47(1):33–186, 1977.

[Mer96] Loïc Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Inventiones mathematicae*, 124(1):437–450, 1996.

[Sil09] Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, 2009.

Licencia Este documento está disponible bajo la licencia Creative Commons CC BY-NC-ND 4.0, que permite su distribución con fines no comerciales, siempre que se otorgue el crédito adecuado y no se realicen obras derivadas.