Ayudantía 7

1. Alturas en curvas elípticas

Sea E una curva elíptica sobre $\mathbb{C}$ junto al punto extra O,

$$E\colon y^2 = x^3 + ax + b.$$

Donde $\Delta = 4a^3 + 27b^2 \neq 0$, esto nos permite asegurar que el polinomio cúbico tiene raíces distintas y así la curva elíptica no es singular.

Sea $f\colon E \to \mathbb{P}^1$ un morfismo sobreyectivo determinado por una función no constante en $\overline{K}(E)$. Así, definimos la altura sobre E (relativa a f) como

$$h_f\colon E(K) \to \mathbb{R}, \qquad h_f(P) = h(f(P)).$$

Ejemplo 1.1: Sea $f = x$, es decir, el morfismo que toma la primera coordenada de los puntos en $E(K)$. Se puede ver que $h_f(O) = 0$, y para $x(P) = p/q \in \mathbb{Q}$

$$h_x(P) = \log \max\{|p|, |q|\}.$$

Teorema 1.2: *Sea K un campo de números. Sea E/K una curva elíptica con las funciones coordenada de Weierstrass x e y, sea $S \subset M_k$ un conjunto finito de valuaciones (tal que contenga las valuaciones arquimedianas). Luego*

$$\{P \in E(K) : v(x(P)) \geq 0 \text{ para cada } v \in M_K \setminus S\}$$

es un conjunto finito.

Ejercicio 1: Sea x la función que toma puntos de la curva elíptica $E(\mathbb{Q})$ y entrega la primera coordenada. Luego, para $P_1, P_2, \ldots \in E(\mathbb{Q})$ puntos racionales ordenados de manera creciente respecto a sus alturas, escribimos

$$x(P_i) = \frac{a_i}{b_i} \in \mathbb{Q}$$

Demuestre que

$$\lim_{i\to\infty} \frac{\log |a_i|}{\log |b_i|} = 1.$$

Este resultado nos permite concluir que las coordenadas x de los puntos racionales de una curva elíptica cumplen que sus numeradores y denominadores tienden a tener aproximadamente el mismo número de dígitos.

2. Dinámicas aritméticas en curvas elípticas

El objeto de estudio en esta ayudantía serán sistemas dinámicos asociados a endomorfimos del grupo multiplicativo $\mathbb{C}^*$.

Si consideramos E vista en el plano proyectivo $\mathbb{P}^2_{\mathbb{C}}$ definida por la ecuación homogénea

$$Y^2Z = X^3 + aXZ^2 + bZ^3,$$

con el punto extra $O = [0 : 1 : 0]$. Existe un automorfismo natural sobre $E(\mathbb{C})$ dado por $[-1](x : y : z) = (x : -y : z)$.

Sea E_1 y E_2 curvas elípticas. Una ***isogenia*** de E_1 a E_2 es un morfismo $f\colon E_1 \to E_2$ tal que $f(O) = O$. Estas satisfacen $f(E_1) = O$ o bien, $f(E_1) = E_2$.

Para cada $m \in \mathbb{Z}$ definimos la isogenia ***multiplicación por m***

$$[d]\colon E \to E,$$

de la manera natural. Entonces, si $d > 0$

$$[d](P) = \underbrace{P + P + \cdots + P}_{d \text{ términos}}.$$

Considerando, además, $[0](P) = 0$ y $[-d](P) = [-1]([d](P))$ se tiene un epimorfismo

$$\mathbb{Z} \to \operatorname{End} E(\mathbb{C}), \qquad d \mapsto [d]$$

si este morfismo no es sobreyectivo, entonces E se dice que tiene ***multiplicación compleja (CM)***. Por ejemplo, $E\colon y^2 = x^3 + x$ tiene multiplicación compleja ya que tiene endomorfismos adicionales tal como $[i]\colon (x, y) \mapsto (-x, iy)$. La mayoría de las curvas no tiene CM.

El mapeo *multiplicación por d* conmuta con la *involución* $[-1]$, así que éste desciende al mapeo cociente $E(\mathbb{C})/\sim$, donde la relación está definida por $P \sim Q$ syss $Q = [-1]P$. Luego, el mapeo cociente está dado por

$$\Phi\colon (E(\mathbb{C})/\sim) \xrightarrow{\sim} \mathbb{P}^1_{\mathbb{C}}, \qquad (x, y) \mapsto x,$$

así que la *multiplicación por d* desciende a darnos un mapeo racional $\phi_{E,d}$ hace que el siguiente diagrama conmute

$$\begin{array}{ccc} E(\mathbb{C}) & \xrightarrow{[d]} & E(\mathbb{C}) \\ \downarrow & & \downarrow \\ \frac{E(\mathbb{C})}{\{\pm 1\}} & \xrightarrow{[d]} & \frac{E(\mathbb{C})}{\{\pm 1\}} \\ \Phi\downarrow & & \downarrow\Phi \\ \mathbb{P}^1_{\mathbb{C}} & \xrightarrow{\phi_{E,d}} & \mathbb{P}^1_{\mathbb{C}} \end{array}$$

El mapeo $\phi_{E,d}$ es un ejemplo de ***mapeo Lattès***. Luego, $\phi_{E,d}$ es una función racional caracterizada por

$$\phi_{E,d}(x(P)) = x([d](P)), \qquad \text{para todo } P \in E(\mathbb{C}).$$

Ejemplo 2.1: Sea $E\colon y^2 = x^3 + ax + b$ una curva elíptica como antes. Entonces el mapeo duplicador $[2]\colon E(\mathbb{C}) \to E(\mathbb{C})$ es la función racional

$$\phi_{E,2}(x) = \frac{x^4 + 2ax^2 - 8bx + a^2}{4x^3 + 4ax + 4b}.$$

Ejercicio 2: Demuestre que $\operatorname{Preper} \phi_{E,d} = x(E(\mathbb{C})_{\text{tors}})$.

Conjetura 1 (Morton-Silverman): Sea $d \geq 2$, y $D \leq 1$. Existe una constande $C_{d,D}$ tal que para cada campo de números K con $[K : \mathbb{Q}] \leq D$ y cada morfismo $\phi\colon \mathbb{P}^1 \to \mathbb{P}^1$ de grado d definida sobre K, tal que

$$\#\operatorname{Preper}(\phi, \mathbb{P}^1_K) \leq C_{d,D}$$

Referencias

1. Silverman, J. H. *The Arithmetic of Elliptic Curves* (Springer Science Business Media, 2009).

Correo electrónico: rseplveda@uc.cl