Teoría de números – MAT2225 Segundo semestre del 2024
Profesor: Héctor Pastén Ayudante: Rocío Sepúlveda Manzo

Ayudantía 7

Sea k un campo. Una ***curva elíptica*** sobre k es una curva proyectiva, suave, con un punto k-racional O isomorfa a una curva de la forma $\mathbb{V}(F) \subseteq \mathbb{P}^2(k)$, donde f es homogéneo de grado 3. Otra forma equivalente de definir una curva elíptica es como una subvariedad suave de $\mathbb{P}^2(k)$ dada por una ecuación:

$$E\colon y^2z + a_1xyz = x^3 + a_2x^2z + a_4xz^2 + a_6z^3,$$

donde $a_1, \ldots, a_6 \in k$ y $O = [0:1:0]$.

Para trabajar la ecuación debemos verla respecto a una carta afín $U_z = \{[x:y:z] \in \mathbb{P}^2 : z = 1\}$ de $\mathbb{P}^2$, obteniendo así

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Luego, la curva elíptica E consiste en los puntos $P = (x, y)$ que satisfacen la ***ecuación de Weierstrass***, notando además que siempre tendremos un punto $O = [0:1:0]$ afuera en el infinito.

Ley de composición 1: *Sean $P, Q \in E$, sea L una línea que cruza P y Q (si $P = Q$ tomamos la línea tangente a E en P), y sea R el tercer punto de intersección de L con E. Sea L' la línea que cruza R y O. Entonces L' intersecta E en R, O y un tercer punto, ese punto lo denotaremos como $P \oplus Q$.*

Observación 1. En general, se simplifica la notación de la suma al símbolo usual $+$.

El conjunto de puntos de E forma un grupo abeliano con la identidad O. Más aún,

$$E(k) = \{(x, y) \in k^2 : y^2 + a_1xy = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\}.$$

Es un subgrupo de E, el cual es *el conjunto de puntos k-racionales de la curva E.*

Teorema 0.1 (Mordell-Weil, 1929): *Sea E una curva elíptica sobre $\mathbb{Q}$. Entonces su grupo de puntos racionales $E(\mathbb{Q})$ es finitamente generado.*

Teorema 0.2 (débil de Lutz-Nagell, 1937): *Sea E una curva elíptica sobre $\mathbb{Q}$ dada por una ecuación de Weierstrass en $\mathbb{P}^2(\mathbb{Q})$. Todos los puntos racionales de torsión tienen coordenadas enteras.*

1. Con SAGE

Ejercicio 1: Encuentre una fórmula para todas las sucesiones de tres cuadrados en progresión aritmética.

Ejercicio 2: Demuestre que no hay cuatro cuadrados en progresión aritmética.

Ejercicio 3: Encuentre todas las sucesiones de tres cubos coprimos en progresión aritmética.

2. Sin SAGE

Ejercicio 4: Encuentre una ecuación de Weierstrass para la curva elíptica $E\colon x^3 + y^3 = z^3$.

Ejercicio 5: Demuestre que la curva elíptica $y^2 = x^3 + x^2 + 4$ tiene infinitas soluciones.

Referencias

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

Correo electrónico: `rseplveda@uc.cl`