Pontificia Universidad Católica de Chile
Facultad de Matemáticas

Profesor: Héctor Pastén
Ayudante: José Cuevas Barrientos
Curso: Teoría de Números
Sigla: MAT2225
Fecha: 24 de noviembre de 2023

Curvas elípticas

1. Con Sage

Una ***curva elíptica*** E sobre un cuerpo k admite varias definiciones equivalentes:

1. Es una curva proyectiva, suave, con un punto k-racional isomorfa a una curva de la forma $\mathbf{V}_+(f) \subseteq \mathbb{P}^2(k)$, donde f es homogéneo de grado 3.
2. Es una subvariedad suave de $\mathbb{P}^2(k)$ dada por una ecuación de Weierstrass:
$$y^2z + a_1xyz = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$
3. Es una curva proyectiva cuyos puntos K-racionales forman un grupo abeliano (en particular, $E(K)$ debe ser no vacío, pues los grupos son no vacíos).

Teorema 1.1 (Mordell-Weil, 1929): Sea E una curva elíptica sobre $\mathbb{Q}$. Entonces su grupo de puntos racionales $E(\mathbb{Q})$ es finitamente generado.

Definición 1.2: Un elemento g de un grupo abeliano G se dice ***de torsión*** si $g + \cdots + g = n \cdot g = 0$ para algún $n \geq 1$.

El siguiente criterio es útil:

Teorema 1.3 (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. Encuentre una fórmula para todas las sucesiones de tres cuadrados en progresión aritmética.
2. Demuestre que no hay cuatro cuadrados en progresión aritmética.
3. Encuentre todas las sucesiones de tres cubos coprimos en progresión aritmética.

2. Sin Sage

4. Encuentre una ecuación de Weierstrass para la curva elíptica $E\colon x^3 + y^3 = z^3$.
5. Demuestre que la curva elíptica $y^2 = x^3 + x^2 + 4$ tiene infinitas soluciones.

Referencias y lecturas adicionales

1. Silverman, J. H. *The arithmetic of elliptic curves* 2.ª ed. (Springer-Verlag, 2009).

Correo electrónico: josecuevasbtos@uc.cl