



Pontificia Universidad Católica de Chile
Facultad de Matemáticas

Profesor: Ricardo Menares
Curso: Teoría de Números
Fecha: 7 de noviembre de 2025

Ayudante: José Cuevas Barrientos
Sigla: MAT2814

Curvas elípticas

1. EJERCICIOS

1. Pruebe que la curva proyectiva $X^3 + Y^3 = Z^3$ es una curva elíptica sobre un cuerpo k de característica $\text{car } k \neq 3$ y dé una ecuación de Weierstrass corta (i.e., de la forma $y^2 = x^3 + ax + b$) cuando $\text{car } k \nmid 6$.
¿Qué falla exactamente en $\text{car } k = 3$?
2. Sea $C: y^2 = f(x) := x^3 + b_2x^2 + b_4x + b_6$ una curva afín con clausura proyectiva \bar{C} .
 - a) Pruebe que posee un único punto $o \in \bar{C}(k) \setminus C(k)$ «al infinito».
 - b) Pruebe que o es un punto suave y, más generalmente, calcule cuales son los posibles puntos singulares. Dé un ejemplo concreto donde efectivamente los puntos que satisfagan esta propiedad sean los singulares.
3. Sea $C: y^2 = f(x)$ una curva elíptica como antes.
 - a) Pruebe que si $P = (x, y)$, entonces tenemos la siguiente fórmula de duplicación

$$x(2P) = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}.$$

PISTA: Recuerde que las relaciones de Viète dicen que si un polinomio cúbico $x^3 + \alpha x^2 + \beta x + \gamma = 0$ tiene raíces r_1, r_2, r_3 , entonces $\alpha = -r_1 - r_2 - r_3$. \square

- b) Concluya que los polinomios $x^4 - 2bx^2 - 8cx + b^2 - 4ac$ y $f(x)$ no tienen raíces comunes (en k^{alg}).
4. Más en general, la cúbica $E: X^3 + Y^3 = \alpha Z^3$ (con $\alpha \neq 0$) tiene un punto racional $o := [1 : -1 : 0] \in E(k)$ al infinito.
 - a) Calcule una fórmula para la suma (con neutro o) $P + Q$ de dos puntos afines distintos $P = (u_1, v_1)$ y $Q = (u_2, v_2)$.
 - b) Encuentre una fórmula de duplicación para el punto afín $P = (u, v)$.
5. Sea $C: y^2 = f(x)$ una curva afín con clausura proyectiva \bar{C} , donde f es un polinomio mónico de $\deg f \geq 3$.
 - a) Pruebe que, en el cuerpo finito \mathbb{F}_p , tenemos la fórmula

$$|C(\mathbb{F}_p)| = p + 1 + \sum_{j=0}^{p-1} \left(\frac{f(j)}{p} \right),$$

donde (a/p) es el símbolo de Legendre.

- b) Muestre que si $f(x) = x^3 + d$; entonces para $p \equiv 2 \pmod{3}$, se cumple que $|C(\mathbb{F}_p)| = p + 1$.
PISTA: Muestre que $x \mapsto x^3$ es un automorfismo de \mathbb{F}_p^\times . \square

REFERENCIAS

1. SILVERMAN, J. H. y TATE, J. *Rational points on elliptic curves* doi:[10.1007/978-1-4757-4252-7](https://doi.org/10.1007/978-1-4757-4252-7) (Springer-Verlag, New York, 1992).

Correo electrónico: josecuevasbtos@uc.cl