

Resumen del Capítulo 4

1. Introducción a las curvas elípticas

¿Cuáles son los resultados importantes?

- La suma de puntos racionales en una curva elíptica tiene estructura de grupo.
- Teorema de Mordell-Weil.
- Teorema de Siegel.

¿Qué se espera de mí? Sobre todo que comprendas cómo aplicar la ley de grupo (sumar puntos) en una curva elíptica escrita en forma canónica, entendiendo el cálculo y su significado geométrico. Los resultados teóricos fundamentales, especialmente el teorema de Mordell-Weil, son de escaso valor en los ejercicios prácticos (de hecho no hay ningún algoritmo fiable para calcular el grupo de Mordell-Weil), aun así los debes conocer.