

Elliptische Kurven als Gruppen

Aufgabe 1. Sei C die Kurve $y^2 = x^3 + 3x + 1$ über dem Körper \mathbb{Z}_5 . Beweisen Sie, dass diese Kurve elliptisch ist und $\widehat{C} \cong \mathbb{Z}_7$ ist. Berechnen Sie ein Erzeugendes dieser Gruppe.

Aufgabe 2. Sei C_b die Kurve $y^2 = x^3 + bx + 1$ über dem Körper \mathbb{Z}_7 . Listen Sie alle möglichen Gruppen \widehat{C}_b . Bestimmen Sie die Struktur dieser Gruppen.