

Elliptische Kurven als Gruppen

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

Aufgabe 3. Finden Sie eine elliptische Kurve ueber \mathbb{Z}_p , die folgende Untergruppe enthält:

- a) $\mathbb{Z}_2 \times \mathbb{Z}_2$,
- b) $\mathbb{Z}_3 \times \mathbb{Z}_3$.