Übungszettel 11

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_a die Kurve $y^2 = x^3 + 2x + a$ über dem Körper $\mathbb{Z}_7$. Finden Sie a, so dass

1) $|C| = 9$,
2) $|C| = 8$

ist

Ob diese Gruppen zyklisch sind?

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