Elliptische Kurven und Kryptographie

Serie 10

elliptische Kurven über endlichen Körpern — Besprechung am 5. Dezember

---

30. Sei $\mathbb{F} := \mathbb{Z}_{13}$ und sei $E = (C, \mathscr{O}, +)$ die elliptische Kurve über dem Körper $\mathbb{F}$ mit

$$C\colon y^2 = x^3 + x^2 + x\,.$$

Zeige: $E \cong \mathbb{Z}_2 \times \mathbb{Z}_8$.

Hinweis: Der Punkt $(2, 1)$ hat die Ordnung 8.

31. Sei $C\colon y^2 + xy = x^3 + a_2x^2 + a_6$ eine cubische Kurve über einem Körper $\mathbb{F}_q$ der Charakteristik 2 und sei $(x_0, y_0) \in C$ mit $x_0 \neq 0$.

(a) Dividiere $y_0^2 + x_0y_0 + x_0^3 + a_2x_0^2 + a_6$ durch x_0^2, setze $x := x_0$ und $u_0 := \frac{y_0}{x_0}$, und schreibe die entsprechende quadratische Gleichung in u_0 auf.

(b) Zeige, dass nebst $u_0 := \frac{y_0}{x_0}$ auch $u_0 + 1$ eine Lösung dieser quadratischen Gleichung ist und finde so einen weiteren Punkt (X_0, Y_1) auf C.

32. Sei $\mathbb{F}_{64} = \mathbb{Z}_2[X]/(X^6 + X^5 + 1)$, sei

$$C\colon y^2 + xy = x^3 + a_2x^2 + a_6$$

eine cubische Kurve über $\mathbb{F}_{64}$, und sei $a_2 := (X^4 + X + 1)$.

(a) Bestimme a_6 so, dass der Punkt

$$\big(X^2 + 1,\ X^3 + X + 1\big)$$

auf C liegt.

(b) Bestimme einen weiteren Punkt (verschieden von $\mathscr{O}$) auf C.