Kryptographie Blatt 11

hhu Düsseldorf
WiSe 2023/24

Abgabe: bis Montag 15.1.2024, vor der Vorlesung

Vorlesungswebseite: `http://reh.math.uni-duesseldorf.de/~khalupczok/krypto/`

Aufgabe 1: Ordnung eines Punktes einer elliptischen Kurve

Sei E die elliptische Kurve über $\mathbb{F}_7$ mit der Gleichung $E : y^2 = x^3 + x + 3$.

(a) Bestimmen Sie die Menge $E(\mathbb{F}_7)$ aller Punkte auf E.

(b) Welche Ordnung hat der Punkt $P = (4, 1) \in E(\mathbb{F}_7)$?

(c) Zeigen Sie, dass $E(\mathbb{F}_7) \cong \mathbb{Z}_6$ ist, d. h. $E(\mathbb{F}_7)$ ist zyklisch der Ordnung 6.

Aufgabe 2: Gruppenstruktur elliptischer Kurven

Seien E_1 und E_2 die elliptischen Kurven über $\mathbb{F}_{11}$ mit den Gleichungen $E_1 : y^2 = x^3 + x + 1$ und $E_2 : y^2 = x^3 + x$. Bestimmen Sie die Gruppenstruktur von $E_1(\mathbb{F}_{11})$ und $E_2(\mathbb{F}_{11})$.

Aufgabe 3: Diskriminantenkriterium

Sei $\mathcal{C}$ eine Kurve über $\mathbb{C}$ mit affiner Gleichung $y^2 = x^3 + ax^2 + bx + c$.
Berechnen Sie die Diskriminante $\Delta(\mathcal{C})$.
Für welche c definiert die Gleichung $y^2 = x^3 - 4x^2 + c$ eine elliptische Kurve $E(\mathbb{C})$?