Kryptologie

Übung, LVA 405.321
C. Fuchs

5. Übungsblatt, SS 2022

06.04.2022

1. Berechne die Ordnung von 5 in den Gruppen $\mathbb{Z}_{49}^{\times}, \mathbb{Z}_{103}^{\times}$ und $\mathbb{Z}_{111}^{\times}$ sowie die Ordnung von X in der multiplikativen Gruppe des endlichen Körpers $\mathbb{Z}_7[X]/(X^2+1)$.

2. Finde alle Elemente der Ordnung 2 in der Gruppe $\mathbb{Z}_{65}^{\times}$ sowie ein Element der Ordnung 10 in $\mathbb{Z}_{121}^{\times}$. Wieviele gibt es?

3. Bestimme alle endlichen Körper $\mathbb{F}_q$, sodass außer $0, 1$ alle Elemente eine Primitivwurzel sind. Wieviele dieser Körper gibt es?

4. Wieviele Primitivwurzeln modulo 31 gibt es? Gib die kleinste Primitivwurzel an und löse damit die Gleichung $2x^{16} \equiv 5 \pmod{31}$.