5. Übung Kryptographie

1. Aufgabe

Zeige folgende Aussagen:

- (i) Sei G eine abelsche Gruppe mit $|G| = p \in \mathbb{P}$. Zeigen Sie, dass G eine zyklische Gruppe ist, d.h. es ist $G = \langle g \rangle$ mit einem geeigneten $g \in G$.
- (ii) Sei G eine nicht-triviale Gruppe und H ein Normalteiler von G für den gilt: $g^2 \in H \forall g \in G$. Sei weiterhin $(G : H) < \infty$. Zeigen Sie, dass dann $(G : H) = 2^j$ ($j \in \mathbb{N} \cup \{0\}$) gilt. Benutzen Sie dazu folgende Aussage ohne Beweis: Ist G eine Gruppe mit $|G| = p \cdot k$ ($p \in \mathbb{P}$), so besitzt G eine Untergruppe der Ordnung p .
- (iii) Sei $G := (\mathbb{Z}/p^k\mathbb{Z})^\times$ ($p \in \mathbb{P}, k \geq 2$) und $J := \{a \in G : a^{p^{k-1}} \equiv 1 \pmod{p^k}\}$. Zeigen Sie, dass $(J, \cdot)$ eine Untergruppe von G ist und $(G : J) \geq p^{k-1}$ gilt.
- (iv) Sei $G := (\mathbb{Z}/9\mathbb{Z})^\times$ und J wie in (iii). Bestimmen Sie $(G : J)$.

(5 Punkte)

2. Aufgabe

Sei $(G, \circ)$ eine Gruppe. Für $n \in \mathbb{N}$ definiere die Abbildung

$$[n] : G \rightarrow G, a \mapsto \underbrace{a \circ \dots \circ a}_n.$$

Beweisen Sie die folgenden Aussagen:

- (a) Ist G abelsch, so ist $[n]$ für alle $n \in \mathbb{N}$ ein Homomorphismus.
- (b) Ist G zyklisch von endlicher Ordnung g , dann ist $[n]$ genau dann ein Isomorphismus, wenn n und g teilerfremd sind. Zeigen sie weiterhin, dass die Inverse ebenfalls von der Form $[m]$ ist.
- (c) Sei $G = (\mathbb{Z}/23\mathbb{Z}^*, \cdot)$ die multiplikative Gruppe von $\mathbb{Z}/23\mathbb{Z}$. Bestimmen sie die inverse Abbildung zu $[5] : G \rightarrow G$.

(5 Punkte)

3. Aufgabe

In Fürstenfeldbruck, einer oberbayrischen Kreisstadt, stehen drei Kirchen: die Erlöserkirche, St. Leonhard Kirche und die Klosterkirche. Die Glocke der Erlöserkirche läutet alle 61 Minuten, die der Leonhard Kirche alle 30 Minuten und die der Klosterkirche alle 7 Minuten.

- (a) Berechnen Sie, wie lange man maximal warten muss, um die Glocken der drei Kirchen gleichzeitig läuten zu hören.
- (b) Angenommen man hat einen Wecker in der Tasche, der alle 20 Minuten läutet. Ermitteln Sie, mit welchen Kirchenglocken der Wecker auf jeden Fall irgendwann mal gleichzeitig läutet.
- (c) Skizzieren Sie eine der Kirchen.

(5 Punkte)

4. Aufgabe

Programmieren Sie den chinesischen Restsatz für $\mathbb{Z}$ gemäß der Anleitung aus der Übung.

(5 Punkte)