Kryptologie

Übung, LVA 405.321
C. Fuchs

6. Übungsblatt, SS 2022

27.04.2022

1. Beweise die Rechenregeln für den Index aus 3.5.6.
2. Zeige, dass $\text{ind}_g(-1) = \varphi(n)/2$ für $n \geq 3$. Folgere, dass es für die Berechnung von $g^l, l \in \{0, 1, \ldots, \varphi(n)-1\}$ genügt, die Werte $g^l, l \in \{0, 1, \ldots, \varphi(n)/2\}$ zu bestimmen.
3. Löse die Kongruenzen $7^x = 6$ in $\mathbb{Z}_{17}$ sowie $2^x = 3$ in $\mathbb{Z}_{23}$.
4. Sei G eine zyklische Gruppe der Ordnung n mit Erzeuger g. Zeige, dass durch $g \mapsto 1$ ein Isomorphismus von G in die additive Gruppe des Restklassenrings mod n gegeben ist. Warum ist das für kryptographische Anwendungen relevant?