# Übungen zur Kryptologie

**Blatt 8** SoS 2024 — H. Kiechle

### Präsenzaufgaben

**23.** Wir rechnen in $\mathbb{Z}_{17}$.

(a) Bestimmen Sie die Elemente der Menge $U = \left\{\overline{2}^k \,;\, k \in \mathbb{Z}\right\}$.

(b) Zeigen Sie, dass $U$ eine Untergruppe von $\mathbb{Z}_{17}^\times$ ist.

(c) Kann das in Aufgabe 24 gesuchte Element $g$ in $U$ liegen? Mit Begründung!

### Hausaufgaben

**24.** Zeigen Sie, dass es in $\mathbb{Z}_{17}^\times$ ein Element $g$ gibt mit $\mathbb{Z}_{17}^\times = \left\{g^k \,;\, k \in \{0, 1, \ldots, 15\}\right\}$.

**Hinweis:** Wenn man $g^2, g^3, \ldots, g^8$ ausgerechnet hat und weiß, dass $g^8 = \overline{-1}$, dann kann man die anderen Potenzen „ablesen“. Wie? Warum?

**25.** Es sei $G = \langle g \rangle$ eine zyklische Gruppe der Ordnung $n$, mit einer geraden Zahl $n \in \mathbb{N}$.

(a) Zeigen Sie, dass genau die Hälfte der Elemente in $G$ Quadrate sind.

(b) Prüfen Sie ob $\mathbb{Z}_8^\times$ eine zyklische Gruppe ist; mit Beweis.

(c) Prüfen Sie ob $\mathbb{Z}_{15}^\times$ eine zyklische Gruppe ist. Nutzen Sie dazu die Ergebnisse aus Aufgabe 19.