

9. Übungsblatt

Abgabe: Freitag, 17. Juni 2018, bis 10.00

Aufgabe 1 Wählen Sie ein $a \in \mathbb{N}$ so, dass $\text{ggT}(a, 561) = 1$ ist, und zeigen Sie mittels des Miller-Rabin Verfahrens, dass die Carmichael-Zahl $n = 561$ keine Primzahl ist.

Aufgabe 2 Zeigen Sie, dass jede Carmichael-Zahl ungerade ist.

Aufgabe 3 Finden Sie eine Primzahllücke der Länge n mit möglichst kleinen Zahlen.
Hinweis: Finden Sie eine möglichst kleine natürliche Zahl N , die durch $2, \dots, n$ geteilt wird und gehen Sie dann wie in der Vorlesung vor.

- Aufgabe 4**
- (a) Sei (G, \circ) eine Gruppe und $g \in G$.
Geben Sie die Definition von $\text{ord}_G(g)$.
 - (b) Sei $(G, \circ) = (\mathbb{Z}_n, +_n)$ für ein $n \in \mathbb{N}, n \geq 2$. Weiter sei $\bar{i} \in \mathbb{Z}_n$.
Wie ist $\text{ord}_{\mathbb{Z}_n}(\bar{i})$ zu berechnen?
 - (c) Sei $(G, \circ) = (\mathbb{Z}_n^*, \cdot_n)$ für ein $n \in \mathbb{N}, n \geq 2$. Weiter sei $\bar{i} \in \mathbb{Z}_n^*$.
Wie ist $\text{ord}_{\mathbb{Z}_n^*}(\bar{i})$ zu berechnen?
 - (d) Berechnen Sie $\text{ord}_{\mathbb{Z}_6}(5)$; $\text{ord}_{\mathbb{Z}_6^*}(5)$, $\text{ord}_{\mathbb{Z}_{12}^*}(5)$ und $\text{ord}_{\mathbb{Z}_{10}}(5)$.