

Aufgabe 10: (6 Punkte)

- (a) Wie lässt sich mit Hilfe des Satzes von Euler die multiplikative Inverse a^{-1} in \mathbb{Z}_n für eine Zahl $a \in \mathbb{Z}_n$ mit $\text{ggT}(a, n) = 1$ berechnen?
Bestimmen Sie auf diese Weise 5^{-1} in \mathbb{Z}_{26} .
- (b) Zeigen Sie: $a^b \bmod n = a^{b \bmod \varphi(n)} \bmod n$ für $a, b, n \in \mathbb{N}^*$ mit $\text{ggT}(a, n) = 1$.
Gilt diese Gleichung auch für Zahlen a mit $\text{ggT}(a, n) \neq 1$?
- (c) Beweisen Sie die Folgerung aus dem Satz von Euler (s. Skript, A.3).

Programmieraufgabe P3: (12 Punkte)

- (a) Implementieren Sie das Sieb des Eratosthenes und bestimmen Sie damit alle Primzahlen im Intervall $[1, 10001]$.
- (b) Implementieren Sie den Fermat-Test. Wenden Sie ihn auf alle zusammengesetzten ungeraden Zahlen $n \in [1, 1001]$ an. Bestimmen Sie für dieses Intervall experimentell den durchschnittlichen und minimalen Anteil von Zeugen unter allen Basen $2 \leq a < n$ bzw. unter allen Basen $2 \leq a < n$ mit $\text{ggT}(a, n) = 1$.
- (c) Implementieren Sie den Rabin-Miller-Test. Wenden Sie ihn auf alle zusammengesetzten ungeraden Zahlen $n \in [1, 1001]$ an. Bestimmen Sie für dieses Intervall experimentell den durchschnittlichen und minimalen Anteil von Zeugen unter allen Basen $2 \leq a < n$ bzw. unter allen Basen $2 \leq a < n$ mit $\text{ggT}(a, n) = 1$.