Zahlentheorie

Übung, LVA 405.031
C. Fuchs, I. Vukusic

13. Übungsblatt, SS 2022

24.06.2022

1. Zeige, dass $m^5 \equiv m \pmod{10}$ für alle ganzen Zahlen m gilt.

2. Im RSA-Verfahren mit öffentlichem Schlüssel (n, e) mit $n = 86267 = 281 \cdot 307$ und $e = 65537$ codiere man die Nachricht $m = 123417$. Bestimme den geheimen Schlüssel d und decodiere im Anschluß wieder.

3. Die Buchstaben A,B,C,...,Z seien wie üblich durch die Zahlen $10, 11, 12, \ldots, 35$ codiert. Verwende das RSA-Verfahren mit den Werten $p = 5, q = 11$ und $e = 3$ und a) verschlüssele die Nachricht MATHE, b) entschlüssele den Geheimtext $26, 50, 24$.

4. Können Sie den RSA-Modul $n = 14803$ faktorisieren, wenn sie wissen, dass $\varphi(n) = 14560$ ist?

5. Sei $n = 323$ und $e = 17$. Berechne den kleinsten Exponenten k, so dass $\gamma^k = \mathrm{id}_{\mathbb{Z}_n}$ für $\gamma : \mathbb{Z}_n \to \mathbb{Z}_n, x \mapsto x^e$.