

ELEMENTARE ZAHLENTHEORIE
8. PRÄSENZBLATT

DR. BAPTISTE ROGNERUD

Aufgabe 1. Zeigen Sie:

- (a) 25 ist 7-*psp*.
- (b) 341 ist 3-*psp* und 341 ist nicht ein Carmichael Zahl.

Aufgabe 2. Satz 55: Sei $a \in \mathbb{N}_{>1}$. Dann gibt es unendlich viele a -*psps*.Zeigen Sie Satz 55 für den Spezialfall $a = 2$, indem Sie den Beweis aus des Vorlesung anpassen.**Aufgabe 3.**

- (a) Alice verschlüsselt die Nachricht m mit dem öffentlichen Schlüssel $(e, n) = (11, 51)$. Der verschlüsselte Text sei 31. Bobs privater Schlüssel sei $(3, 51)$. Bestimme, falls möglich, den Klartext.
- (b) Alice verschlüsselt die Nachricht m mit dem öffentlichen Schlüssel $(7, 33)$. Der verschlüsselte Text sei 9. Bobs privater Schlüssel sei ebenfalls $(33, 3)$. Bestimme, falls m möglich, den Klartext.

Aufgabe 4.

- (a) Berechnen Sie die Ordnung von den Gruppenelementen von $(\mathbb{Z}/9\mathbb{Z})^\times$
- (b) Ist $(\mathbb{Z}/9\mathbb{Z})^\times$ eine zyklische Gruppe?