F. Stoll **12. Übungsblatt zur Vorlesung** W. Kimmerle

Mathematische Grundlagen für das Lehramt

Winter 2013/14

Aufgabe 39.
Stellen Sie die Mutliplikationstabelle von $\mathbb{Z}_{12}^*$.

Aufgabe 40.

(a) Verschlüsseln Sie die Zahl 8 mit Hilfe des RSA-Verfahrens mit $n = 55$, $e = 7$.

(b) Finden Sie $d \in \mathbb{N}$ mit $ed \equiv 1 \mod \varphi(n)$ und verifizieren Sie, dass die Entschlüsselung funktioniert.

(c) Warum ist es schlecht, Daten in der Wirklichkeit mit $n = 55, e = 7$ zu verschlüsseln?

Aufgabe 41.

(a) Zeigen Sie: Ist p eine Primzahl und $n \in \mathbb{N}$, dann ist $\varphi(p^n) = p^{n-1}(p-1)$.

(b) Bestimmen Sie alle $n \in \mathbb{N}$ mit $\varphi(n) = 16$.

(c) Zeigen Sie, dass es kein $n \in \mathbb{N}$ gibt mit $\varphi(n) = 14$.

Aufgabe 42.
Sei G eine endliche abelsche Gruppe mit neutralem Element e. Sei $g \in G$ mit Ordnung $\mathrm{ord}(g)$. Zeigen Sie, dass $g^m = g^n$ genau dann gilt, wenn $m \equiv n \mod \mathrm{ord}(g)$ ist.