

**Aufgabe 2.1** Berechnen Sie die Ordnungen folgender Gruppenelemente:

(a)  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 2 & 6 & 8 & 9 & 1 & 3 & 7 & 5 \end{pmatrix} \in S_9$

(b)  $\bar{7} \in \mathbb{Z}/120$

(c)  $\bar{7} \in (\mathbb{Z}/120)^*$

(d) die Drehmatrix  $D_\alpha = \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix} \in \text{GL}_2(\mathbb{R})$  für  $\alpha = 30^\circ$  und  $\alpha = 17^\circ$

**Aufgabe 2.2** Geben Sie alle Einheiten im Matrizenring  $M(2, \mathbb{F}_2)$  an.

**Aufgabe 2.3** Berechnen Sie die modulare Potenz  $13^{77777} \in \mathbb{Z}/543$  ohne Hilfsmittel mit dem Satz von Euler.

**Aufgabe 2.4** Wir wollen Ver- und Entschlüsselung im RSA-Algorithmus an einem kleinen Beispiel testen, mit  $p = 61$ ,  $q = 79$ ,  $e = 127$ .

Sie können hier und für Aufgabe 2.5 Hilfsmittel für die modulare Arithmetik benutzen, wie zum Beispiel <http://ptrow.com/perl/calculator.pl>.

(a) Berechnen Sie  $n = pq$  und  $\varphi(n)$  und den Entschlüsselungsexponenten  $d$  ( $de \equiv 1 \pmod{\varphi(n)}$ ),

(b) Verschlüsseln Sie die Nachrichten  $N = 2$  und  $N = 222$ .

(c) Entschlüsseln Sie die in (b) erhaltenen Codes.

**Aufgabe 2.5** Führen Sie das RSA-Verfahren zusammen mit einem Kommilitonen durch.

(a) Wählen Sie Primzahlen  $p, q > 1000$  und berechnen Sie  $n$  und  $\varphi(n)$

(b) Wählen Sie einen Verschlüsselungsexponent  $e > 100$  mit  $\text{ggT}(e, \varphi(n)) = 1$ .

(b) Berechnen Sie den Entschlüsselungsexponenten  $d$ .

(d) Geben Sie den öffentlichen Schlüssel  $(n, e)$  an Ihren Kommilitonen.

(e) Lassen Sie sich eine verschlüsselte Nachricht schicken.

(f) Entschlüsseln Sie diese Nachricht und vergleichen Sie!

(x) Nehmen Sie den öffentlichen Schlüssel  $(n', e')$  Ihres Kommilitonen und eine kodierte Nachricht  $c \in \mathbb{Z}/n$ . Was müssten Sie tun, um  $c$  zu entschlüsseln?