Aufgabe: Sei G eine Gruppe. Beweisen oder widerlegen Sie:

$$C(G) := \{x \in G \mid xg = gx \text{ für alle } g \in G\}$$

ist eine Untergruppe von G.

Zur Erinnerung: Eine Algebra $\langle G, \circ \rangle$ ist genau dann eine Gruppe, falls

- das Assoziativgesetz gilt,
- es ein neutrales Element gibt und
- jedes Element ein Inverses hat.

Um zu zeigen, dass H eine Untergruppe von G ist, ist nachzuprüfen, dass

- $H \subseteq G$,
- H bezüglich der Gruppenoperation $\circ$ abgeschlossen ist.

Aufgabe: Sei G eine endliche Gruppe und $b \in G$ beliebig. Dann gilt:

$$\text{ord}(b^t) = \frac{\text{ord}(b)}{\text{ggT}(\text{ord}(b), t)}.$$

Aufgabe: Bestimme das Inverse von 348 in Z_{1481}.

Zur Erinnerung:

Das Inverse zu einer Zahl $a \in \mathbb{Z}_n$ ist eine Zahl $x \in \mathbb{Z}_n$ mit $(a \cdot x \text{ mod } n) = 1$.

Frage: Wann gibt es zu jeder Zahl $a \in \mathbb{Z}_n$ ein Inverses?

Antwort: Genau dann wenn n eine Primzahl ist. (1481 is Primzahl.)

Frage: Wie bestimmt man ein Inverses?

Antwort: Mit dem erweiterten Euklidischen Algorithmus:

- Dieser bestimmt für zwei Zahlen $m, n \in \mathbb{N}$ Zahlen $x, y \in \mathbb{Z}$ mit ggT$(m, n) = xm + yn$.
- Sind a, n Zahlen mit ggT$(a, n) = 1$ und x, y die Zahlen des erweiterten Euklidischen Algorithmus (ggf. so modifiziert, dass $x \in \mathbb{Z}_n$), so ist x das Inverse von a.

Aufgabe: Beweise, dass für alle Primzahlen p gilt:

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

Aufgabe: Beweisen oder widerlegen Sie:

Für alle Primzahlen p gilt:

$$\{a \in \mathbb{Z}_p^* \mid a^{-1} = a\} = \{1, p-1\}.$$

Zur Erinnerung:

Satz von Fermat:

$$n \text{ Primzahl} \iff a^{n-1} \equiv 1 \pmod{n} \quad \text{für alle } a \in \mathbb{Z}_n \setminus \{0\}.$$

Satz: Für alle Elemente $a \in G$ gilt: Die Ordnung von teilt die Kardinalität der Gruppe. Also $\text{ord}(a) \mid |G|$.

Satz: Für alle Primzahlen p gilt: $\mathbb{Z}_p^*$ ist zyklisch, d.h. es gibt ein $b \in \mathbb{Z}_p^*$ mit

$$\{b, b^2, b^3, \ldots, b^{p-1}\} = \mathbb{Z}_p^*.$$

Aufgabe: Beweisen oder widerlegen Sie: Sind p und q zwei Primzahlen, so gilt $\phi(pq) = (p-1)(q-1)$.

Zur Erinnerung:

- *Eulersche Phi-Funktion*: $\phi(n) := |\mathbb{Z}_n^*|$,
  wobei
  $$\mathbb{Z}_n^* = \{a \mid a \in \mathbb{Z}_n \setminus \{0\}, \text{ggT}(a, n) = 1\}.$$
- Chinesischer Restsatz: Für alle natürlichen Zahlen $m, n \in \mathbb{N}$ mit $\text{ggT}(m, n) = 1$ und alle $a \in \mathbb{Z}_m$ und $b \in \mathbb{Z}_n$ gibt es ein eindeutig bestimmtes $t \in \mathbb{Z}_{mn}$ so dass
  $$\begin{aligned} t &\equiv a \pmod{m} \quad \text{und} \\ t &\equiv b \pmod{n}. \end{aligned}$$

Aufgabe: Bestimmen Sie ein primitives Element in $\mathbb{Z}_2[x]/(x^3 + x^2 + 1)$.

Zur Erinnerung:

- Ein *primitives Element* eines endlichen Körpers K ist ein Generator der multiplikativen Gruppe von K. D.h.,

$$\alpha \text{ primitives Element} \qquad \Longleftrightarrow \qquad K \setminus \{0\} = \{\alpha, \alpha^2, \ldots, \alpha^{|K|-1}\}.$$

- **Satz:** Jeder endliche Körper enthält ein primitives Element.

- $K[x]/\pi(x) = \{[f(x)]_\pi \mid f(x) \text{ Polynom in } K[x] \text{ mit grad}(f) < \text{grad}(\pi)\}$.
  Also

$$\mathbb{Z}_2[x]/(x^3 + x^2 + 1) = \{[0], [1], [x], [x+1], [x^2], [x^2+1], [x^2+x], [x^2+x+1]\}.$$