Tr 1. Seien $n \in \mathbb{N}$, $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{Z}$. Zeigen Sie durch Induktion nach n: Ist $a_i \equiv b_i \mod m$ für alle $i \in [1, n]$, so folgt $a_1 \cdots a_n \equiv b_1 \cdots b_n \mod m$.

Tr 2. Sei $m \in \mathbb{N}$. Ist $R \subset \mathbb{Z}$ ein vollständiges Restsystem modulo m und $a \in \mathbb{Z}$, so ist auch $a + R = \{ a + r \mid r \in R \}$ ein vollständiges Restsystem modulo m.

Ü 1. Bestimmen Sie jeweils alle $x \in \mathbb{Z}$, die folgende lineare Kongruenzen erfüllen:

(a) $3x \equiv 5 \mod 10$, (b) $2x \equiv 4 \mod 8$, (c) $52x \equiv 135 \mod 87$.

Ü 2. Bestimmen Sie die letzten beiden Dezimalziffern von 9^{9^9}. (*Hinweis:* Zeigen Sie zuerst $9^9 = 9 + 10k$ mit $k \in \mathbb{N}_0$ und betrachten Sie 9^{10} modulo 100.)

Ü 3. Im einheitlichen Euro-Zahlungsverkehrsraum werden Kontonummern im IBAN Format angegeben. Jede solche IBAN enthält eine Prüfsumme, die gegen die häufigsten Formen von Tipp- bzw. Übertragungsfehlern schützen soll.

(1) Informieren Sie sich über den Aufbau einer IBAN und das Verfahren zum Bestimmen der Prüfsumme.

(2) Überprüfen Sie, dass die folgende IBAN den Konventionen für eine österreichische IBAN entspricht und eine gültige Prüfsumme aufweist:

AT69 1904 3000 0001 2507

(Das ist leider notwendigerweise ein wenig rechenaufwendig. Versuchen Sie durch geschicktes Ausnutzen der Rechenregeln für Kongruenzen den Aufwand möglichst gering zu halten.)

(3) Beweisen Sie, dass durch die Prüfsumme folgende Fehler stets entdeckt werden:

- Falsche Eingabe eines einzelnen Zeichens.
- Einmaliges Vertauschen von zwei benachbarten Zeichen.

Für die folgenden Aufgaben ist Stoff aus der Vorlesungseinheit vom 6.12. hilfreich (insbesondere Restklassenringe).

Tr 3. Sei R ein Ring und $a \in R$ eine Einheit. Zeigen Sie, analog dem Beweis für Gruppen, dass das multiplikativ inverse Element von a eindeutig bestimmt ist.

Ü 4. Für eine endliche Menge $\emptyset \neq M$ und eine Verknüpfung $*\colon M \times M \to M$ kann man eine *Verknüpfungstafel* aufschreiben: Hierbei handelt es sich um einen Tabelle, deren Spalten und Zeilen jeweils den Elementen von M entsprechen. Im Eintrag zur Zeile $m \in M$ und Spalte $n \in N$ steht das Verknüpfungsergebnis $m * n$.

Bestimmen Sie die Verknüpfungstafeln für $(\mathbb{Z}/6\mathbb{Z}, +)$ und $(\mathbb{Z}/6\mathbb{Z}, \cdot)$. Welche Eigenschaften können Sie direkt aus der Verknüpfungstafel ablesen?

Tr 4. Sei R ein Ring. Ein Element $a \in R$ heißt *kürzbar* wenn gilt: Sind $b, c \in R$ mit $ab = ac$ oder $ba = ca$, so folgt $b = c$. Zeigen Sie: Jedes invertierbare Element von R ist kürzbar.

Ü 5. (1) Ist $p \in \mathbb{P}$ und $x \in \mathbb{Z}$, so ist $x^2 \equiv 1 \mod p$ genau dann wenn $x \equiv 1 \mod p$ oder $x \equiv -1 \mod p$.

(2) Für $p \in \mathbb{P}$ gilt $(p-2)! \equiv 1 \mod p$.

(*Hinweis:* Arbeiten Sie im Restklassenring $\mathbb{Z}/p\mathbb{Z}$ und gruppieren Sie die Elemente des Produkts in Paare α, α^{-1}.)

(3) (*Satz von Wilson*) Sei $m \in \mathbb{N}_{\geq 2}$. Dann ist m genau dann eine Primzahl, wenn gilt $(m-1)! \equiv -1 \mod m$.