**Aufgabe 35.** Zeige, dass die folgende Aussage wahr ist:

$$a \equiv b \mod m \text{ und } a \equiv b \mod n \implies a \equiv b \mod k \quad \text{für} \quad k = \mathrm{kgV}(m_1, m_2)\,.$$

Ist insbesondere $\mathrm{ggT}(m_1, m_2) = 1$, dann gilt also $a \equiv b\ (m_1 m_2)$.
Folgere daraus, daß die Menge aller Lösungen eines Kongruenzgleichungssystems $x \equiv c_i \mod m_i$, $i = 1, 2, \ldots, k$ und $\mathrm{ggT}(m_i, m_j) = 1$, gegeben ist durch $\{x_0 + km \mid k \in \mathbb{Z}\}$, wobei $m = m_1 m_2 \cdots m_k$.

**Aufgabe 36.** Welche der folgenden Gleichungssystems sind lösbar? Wenn ja, dann bestimme diese. Ist der chinesische Restsatz anwendbar?

$$(a)\quad \begin{aligned} x &\equiv 2 \mod 3 \\ x &\equiv 2 \mod 9 \\ x &\equiv 1 \mod 10 \end{aligned} \qquad (b)\quad \begin{aligned} x &\equiv 1 \mod 5 \\ x &\equiv 3 \mod 9 \\ x &\equiv 2 \mod 10 \end{aligned}$$

**Aufgabe 37.** Berechne ohne Taschenrechner

$$2^{32} \mod 1260$$

*Hinweis*: $1260 = 4 \cdot 5 \cdot 7 \cdot 9$. Rechne zuerst modulo 4, 5, 7, 9 (Regeln fürs Exponentialrechnen ausnützen, es ist fast nichts zu tun!) und wende am Ende den Chinesischen Restsatz an.

**Aufgabe 38.** Welche der folgenden Strukturen $(X, \circ)$ bilden Halbgruppen, Monoide, Gruppen? In welchen gilt das Kommutativgesetz? Bestimme ggf. das neutrale Element, die invertierbaren Elemente und die jeweiligen Inversen.

a. $(\mathbb{Q}, \circ)$ mit $x \circ y = x + 2y$
b. $(\mathbb{N}, \circ)$ mit $x \circ y = \max(x, y)$.
c. $(\mathbb{N}, \circ)$ mit $x \circ y = \min(x, y)$.
d. $(\mathbb{N}_0, \circ)$ mit $x \circ y = |x - y|$.
e. $(\mathbb{R} \setminus \{-1\}, \circ)$ mit $x \circ y = x + y + xy$.
f. $X$ beliebig, $x \circ y = x$.

**Aufgabe 39.**

(a) Berechne $\varphi(10!) = \varphi(2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10)$.
(b) Berechne $\varphi(5186)$, $\varphi(5187)$, $\varphi(5188)$.
(c) Finde alle $n \in \mathbb{N}$ mit $\varphi(n) = 1$.
(d) Finde alle $n \in \mathbb{N}$ mit $\varphi(n) = 2$.
(e) Finde alle $n \in \mathbb{N}$ mit $\varphi(n) = 3$.

*Hinweis*: Wenn $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$, dann ist jedes $\varphi(p_i^{k_i})$ ein Teiler von $\varphi(n)$.

**Aufgabe 40.** Berechne (ohne Taschenrechner), mit Hilfe des Satzes von Euler-Fermat die Potenz

$$2^{(2^{32})} \mod 11\,.$$

**Aufgabe 41.** Berechne mit dem Satz von Euler-Fermat (ohne Taschenrechner) in $\mathbb{Z}_{60}$

$$[14]^{(2^{32})}$$

*Hinweis*: Der Satz von Euler-Fermat ist nicht sofort anwendbar (warum?). Man kann aber wie folgt vorgehen: Zerlege $60 = 2^2 \cdot 3 \cdot 5$. Bestimme $[14]^{(2^{32})} \mod 4$, $[14]^{(2^{32})} \mod 3$, $[14]^{(2^{32})} \mod 5$, und verwende den chinesischen Restsatz, um daraus $14^{(2^{32})} \mod 60$ zu bestimmen.