Diskrete Mathematik für Lehramt Informatik
Sommersemester 2021

9. Übungsblatt (27.5.2021)

Beispiel 9.1. Welche der folgenden Elemente von $\mathbb{Z}_{63}$ sind invertierbar? Bestimmen Sie jeweils das Inverse oder begründen Sie, warum es nicht existiert.

$$[11]_{63}, \quad [18]_{63}, \quad [42]_{63} \quad \text{und} \quad [44]_{63}.$$

Stellen Sie das Inverse, falls es existiert, jeweils in der Form $[b]_{63}$ mit $b \in \{0, 1, \ldots, 62\}$ dar.

Beispiel 9.2. Bestimmen Sie für die folgenden simultanen Kongruenzen jeweils alle Lösungen oder begründen Sie, warum es keine Lösungen gibt.

(a)
$$\begin{aligned} x &\equiv 3 \bmod 5 \\ x &\equiv 1 \bmod 7 \\ x &\equiv 4 \bmod 8 \end{aligned}$$

(b)
$$\begin{aligned} x &\equiv 2 \bmod 3 \\ x &\equiv 1 \bmod 4 \\ x &\equiv 5 \bmod 8 \\ x &\equiv 5 \bmod 9 \end{aligned}$$

Beispiel 9.3. Ermitteln Sie für die folgenden simultanen Kongruenzen jeweils alle Lösungen oder begründen Sie, warum es keine Lösungen gibt.

(a)
$$\begin{aligned} x &\equiv 15 \bmod 28 \\ x &\equiv 3 \bmod 36 \\ x &\equiv 57 \bmod 63 \end{aligned}$$

(b)
$$\begin{aligned} x &\equiv 6 \bmod 28 \\ x &\equiv 10 \bmod 36 \\ x &\equiv 19 \bmod 63 \end{aligned}$$

Hinweis. Finden Sie zuerst Zahlen m_1, m_2, m_3, die relativ prim sind (also $\mathrm{ggT}(m_i, m_j) = 1$ wann immer $i \neq j$) und $28 = m_1 m_2$, $36 = m_1 m_3$ und $63 = m_2 m_3$ erfüllen. Übersetzen Sie dann, falls möglich, die Kongruenzen aus der Aufgabe in die Form

$$\begin{aligned} x &\equiv c_1 \bmod m_1 \\ x &\equiv c_2 \bmod m_2 \\ x &\equiv c_3 \bmod m_3 \end{aligned}$$

und lösen Sie diese mit Hilfe des chinesischen Restsatzes.

Beispiel 9.4. Berechnen Sie ohne Taschenrechner eine Zahl $x \in \{0, 1, \ldots, 1359\}$ mit

$$x \equiv 2^{32} \bmod 1360.$$

Hinweis. $1360 = 5 \cdot 16 \cdot 17$. Finden Sie zuerst Zahlen $c_1 \in \{0, 1, \ldots, 4\}$, $c_2 = \{0, 1, \ldots, 15\}$ und $c_3 = \{0, 1, \ldots, 16\}$ mit

$$[2^{32}]_5 = [c_1]_5, \qquad [2^{32}]_{16} = [c_2]_{16}, \qquad [2^{32}]_{17} = [c_3]_{17}$$

und wenden Sie danach den chinesischen Restsatz an.