Zum Chinesichen Restsatz

Es sei $k \in \mathbb{N}$. Weiter seien $m_1, \ldots, m_k$ paarweise teilerfremd und $a_i \in \{0, \ldots, m_i - 1\}$ für $i = 1, \ldots, k$. Das System von Kongruenzen

$$\begin{aligned} x &\equiv a_1 \bmod m_1 \\ &\vdots \\ x &\equiv a_k \bmod m_k \end{aligned}$$

hat die Lösung

$$x = (m_1 \ldots m_k) \cdot \sum_{i=1}^{k} n_i \frac{a_i}{m_i}.$$

Für $i = 1, \ldots, k$ ist dabei $n_i \in \{1, \ldots, m_i - 1\}$ eindeutig durch

$$n_i \cdot \frac{m_1 \ldots m_k}{m_i} \equiv 1 \bmod m_i$$

bestimmt. Ist y eine weitere Lösung, so gilt

$$y = x + k \cdot (m_1 \ldots m_k)$$

für ein geeignetes $k \in \mathbb{Z}$.

In Aufgabe 1 (Übungsblatt 6) soll zum Beispiel eine spezielle Lösung von

$$\begin{aligned} x &\equiv 4 \bmod 5 \\ x &\equiv 5 \bmod 8 \\ x &\equiv 3 \bmod 7 \\ x &\equiv 2 \bmod 9 \end{aligned}$$

gefunden werden. In diesem Fall gilt also $m_1 = 5$, $m_2 = 8$, $m_3 = 7$ und $m_4 = 9$.

Als erstes wollen wir für $i = 1, \ldots, 4$ nun n_i bestimmen, das heißt die Inversen von $\frac{m_1 \ldots m_4}{m_i}$ modulo m_i.

$$7 \cdot 8 \cdot 9 \equiv 2 \cdot 3 \cdot 4 \bmod 5 \equiv 4 \bmod 5,$$

also erhalten wir aus

$$4 \cdot 4 \equiv 16 \bmod 5 \equiv 1 \bmod 5,$$

daß $n_1 = 4$ gilt. Analog ergibt sich $n_2 = 3$, $n_3 = 5$ und $n_4 = 1$.

Somit läßt sich eine erste Lösung x_0 durch

$$\begin{aligned} x_0 &= 4 \cdot 4 \cdot 8 \cdot 7 \cdot 9 + 5 \cdot 3 \cdot 5 \cdot 7 \cdot 9 + 3 \cdot 4 \cdot 5 \cdot 8 \cdot 9 + 2 \cdot 1 \cdot 5 \cdot 8 \cdot 7 \\ &= 8064 + 4725 + 5400 + 560 \\ &= 18749 \end{aligned}$$

berechnen. Wegen $5 \cdot 8 \cdot 7 \cdot 9 = 2520$ ist $x \in \{18749 + k \cdot 2520 \mid k \in \mathbb{Z}\}$. Da außerdem $0 < x \leq 3333$ gelten soll, erhalten wir schließlich $x = 1109$.