Chinesischer Restsatz

Für teilerfremde natürliche Zahlen $p_1, \ldots, p_n$ besitzen die Kongruenzen

$$\begin{aligned} x &= a_1 \bmod p_1 \\ &\ldots \\ x &= a_n \bmod p_n \end{aligned}$$

genau eine Lösung $x \in \{0, \ldots, P-1\}$, $P = p_1 \cdots p_n$.
Bezeichnet Q_k eine zu $P_k = P/p_k$ inverse ganze Zahl modulo p_k, d.h. ist

$$Q_k P_k = 1 \bmod p_k \,,$$

so gilt

$$x = \sum_{k=1}^{n} a_k Q_k P_k \bmod P \,.$$

Beweis

(i) Existenz:

Darstellung

$$x = \sum_{k=1}^{n} a_k Q_k P_k \mod P$$

$\Longrightarrow$

$$x \mod p_\ell = a_\ell Q_\ell P_\ell \mod p_\ell \,,$$

da p_ℓ Teiler von P_k für $k \neq \ell$

Definition einer zu P_ℓ inversen Zahl Q_ℓ modulo p_ℓ: $Q_\ell P_\ell = 1 \mod p_\ell$

$\Longrightarrow$

$$x = a_\ell \cdot 1 \mod p_\ell = a_\ell \mod p_\ell$$

(ii) Eindeutigkeit:
zu zeigen:

$$x = x' \text{ mod } p_k \text{ für } k = 1, \ldots, n \quad \Longrightarrow \quad x - x' = mP$$

sukzessives Betrachten der Kongruenzen
$x = x' \text{ mod } p_1 \implies$

$$x - x' = m_1 p_1$$

$x = x' \text{ mod } p_2 \quad \Longrightarrow$

$$m_1 p_1 = 0 \text{ mod } p_2 \quad \Longleftrightarrow \quad m_1 p_1 = s p_2$$

p_1, p_2 teilerfremd $\quad \Longrightarrow \quad p_2$ teilt m_1, d.h.

$$m_1 = m_2 p_2, \quad x - x' = m_2 p_1 p_2$$

weitere Kongruenzen $\quad \rightsquigarrow$

$$x - x' = m_3 p_1 p_2 p_3, \ldots, x - x' = m_n p_1 \cdots p_n$$

Beispiel

Bestimmung einer Lösung x der Kongruenzen

$$\begin{aligned} x &= 6 \bmod 9 \\ x &= 5 \bmod 10 \\ x &= 4 \bmod 13 \end{aligned}$$

Chinesischer Restsatz $\Longrightarrow$

$$x = 6\,Q_1P_1 + 5\,Q_2P_2 + 4\,Q_3P_3 \bmod P, \quad P = 9 \cdot 10 \cdot 13 = 1170$$

mit

$$P_1 = 10 \cdot 13 = 130, \quad P_2 = 9 \cdot 13 = 117, \quad P_3 = 9 \cdot 10 = 90$$

und Q_k der zu P_k inversen natürlichen Zahl modulo p_k, d.h.

$$Q_kP_k + yp_k = 1$$

Bestimmung der Modulo-Inversen

- Q_1:

$$\begin{aligned} \underline{130} &= 14 \cdot \underline{9} + \underline{4} \\ \underline{9} &= 2 \cdot \underline{4} + 1 \end{aligned}$$

Rückwärtseinsetzen $\rightsquigarrow$

$$\begin{aligned} 1 &= 9 - 2 \cdot 4 \\ &= 9 - 2 \cdot (130 - 14 \cdot 9) = 29 \cdot 9 + (-2)130 \end{aligned}$$

$$\Longrightarrow \quad Q_1 = (-2) \bmod 9 = 7$$

- Q_2:

$$\begin{aligned} \underline{117} &= 11 \cdot \underline{10} + \underline{7} \\ \underline{10} &= 1 \cdot \underline{7} + \underline{3} \\ \underline{7} &= 2 \cdot \underline{3} + 1 \end{aligned}$$

Rückwärtseinsetzen $\rightsquigarrow$

$$\begin{aligned} 1 &= 7 - 2 \cdot 3 \\ &= 7 - 2 \cdot (10 - 1 \cdot 7) = 3 \cdot 7 - 2 \cdot 10 \\ &= 3 \cdot (117 - 11 \cdot 10) - 2 \cdot 10 = 3 \cdot 117 - 35 \cdot 10 \end{aligned}$$

$$\Longrightarrow \quad Q_2 = 3 \bmod 10 = 3$$

- Q_3:

$$\begin{aligned} \underline{90} &= 6 \cdot \underline{13} + \underline{12} \\ \underline{13} &= 1 \cdot \underline{12} + 1 \end{aligned}$$

Rückwärtseinsetzen $\rightsquigarrow$

$$\begin{aligned} 1 &= 13 - 1 \cdot 12 \\ &= 13 - 1 \cdot (90 - 6 \cdot 13) = 7 \cdot 13 + (-1) \cdot 90 \end{aligned}$$

$$\Longrightarrow \quad Q_3 = (-1) \bmod 13 = 12$$

Einsetzen in die Darstellung der Lösung

$$\begin{aligned} x &= 6Q_1P_2 + 5Q_2P_2 + 4Q_3P_3 \bmod 1170 \\ &= 6 \cdot 7 \cdot 130 + 5 \cdot 3 \cdot 117 + 4 \cdot 12 \cdot 90 \bmod 1170 \\ &= 11535 \bmod 1170 = 1005 \end{aligned}$$