KRY: Wahlfach Kryptologie
Lösungen zum 3. Aufgabenblatt

Aufgabe 2
Vorberechnungen für die Anwendung des chinesischen Restsatzes:
$M_1 = m_2 \cdot m_3 = 22 \cdot 391 = 8602$
$M_2 = m_1 \cdot m_3 = 15 \cdot 391 = 5865$
$M_3 = m_1 \cdot m_2 = 15 \cdot 22 = 330$
$u_1 = M_1^{-1} (\text{mod } m_1) = 8602^{-1} (\text{mod } 15) = 13$
$u_2 = M_2^{-1} (\text{mod } m_2) = 5865^{-1} (\text{mod } 22) = 17$
$u_3 = M_3^{-1} (\text{mod } m_3) = 330^{-1} (\text{mod } 391) = 141$

Die Zahl x mit

$$\begin{array}{rcll} x & = & 2 & (\text{mod } 15) \\ x & = & 6 & (\text{mod } 22) \\ x & = & 121 & (\text{mod } 391) \end{array}$$

ist (gemäss der im Skript angegebenen Formel) also gleich

$$c_1 \cdot u_1 \cdot M_1 + c_2 \cdot u_2 \cdot M_2 + c_3 \cdot u_3 \cdot M_3 = 2 \cdot 13 \cdot 8602 + 6 \cdot 17 \cdot 5865 + 121 \cdot 141 \cdot 330 = 512 \ (\text{mod } 15 \cdot 22 \cdot 391)$$

Die gesendete Nachricht ist damit gleich $x^{1/3} = 512^{1/3} = 8$.

Aufgabe 3
Auflistung der Bedingungen

$$\begin{array}{ll} (1) & n = 1 \pmod 2 \\ (2) & n = 1 \pmod 3 \\ (3) & n = 1 \pmod 4 \\ (4) & n = 2 \pmod 5 \end{array}$$

Die Moduln 2 und 4 sind nicht teilerfremd. Gleichung (1) ist somit überflüssig, da sie in (3) enthalten ist.

Nun kann man den chinesischen Restatz anwenden mit $m_1 = 3$, $m_2 = 4$, $m_3 = 5$ und $a_1 = 1$, $a_2 = 1$, $a_3 = 2$. Hilfsberechnungen:

$M_1 = m_2 \cdot m_3 = 5 \cdot 5 = 20$
$M_2 = m_1 \cdot m_3 = 3 \cdot 5 = 15$
$M_3 = m_1 \cdot m_2 = 3 \cdot 4 = 12$
$u_1 = M_1^{-1} (\text{mod } m_1) = 20^{-1} (\text{mod } 3) = 2$
$u_2 = M_2^{-1} (\text{mod } m_2) = 15^{-1} (\text{mod } 4) = 3$
$u_3 = M_3^{-1} (\text{mod } m_3) = 12^{-1} (\text{mod } 5) = 3$

Gemäss der Formel aus dem Skript beträgt die Anzahl Personen

$$a_1 \cdot u_1 \cdot M_1 + a_2 \cdot u_2 \cdot M_2 + a_3 \cdot u_3 \cdot M_3 = 1 \cdot 2 \cdot 20 + 1 \cdot 3 \cdot 15 + 2 \cdot 3 \cdot 12 = 37 \, (\text{mod } 60)$$