EZT Übungsblatt 7

1.)

(1) gesucht: $u \in \mathbb{Z}$ sd. $35 \cdot u \equiv 1 \pmod{41}$

$\Rightarrow$ löse $35 \cdot u + 41 \cdot v = 1$ über $\mathbb{Z}^2$

$41 = 1 \cdot \underline{35} + \underline{6}$

$35 = 5 \cdot \underline{6} + \underline{5}$

$6 = 1 \cdot \underline{5} + \underline{1}$

$5 = 5 \cdot \underline{1} + 0$

$\Rightarrow ggT(41, 35) = 1$ $\Rightarrow$ Inverses existiert (naja, 41 sowieso prim)

$1 = \underline{6} - 1 \cdot \underline{5} = \underline{41} - 1 \cdot \underline{35} - 1 \cdot (\underline{35} - 5 \cdot \underline{6})$

$= \underline{41} - 1 \cdot \underline{35} - 1 \cdot 35 + 5 \cdot (\underline{41} - 1 \cdot \underline{35})$

$= 6 \cdot 41 - 7 \cdot 35$ $\checkmark_{\text{Probe}}$

$\Rightarrow u = -7$ ist (eine) Lösung

$\Rightarrow$ kanonischer Repräsentant ist $x' = -7 + 41 = 34$

(2) löse $6 \cdot u + 35 \cdot v = 1$

$35 = 5 \cdot \underline{6} + \underline{5}$

⋮

siehe oben

$\Rightarrow ggT(35, 6) = 1$

$1 = \underline{6} - 1 \cdot \underline{5} = \underline{6} - 1 \cdot (\underline{35} - 5 \cdot \underline{6}) = 6 \cdot \underline{6} - 1 \cdot \underline{35}$

$\Rightarrow u = 6$ ist (eine) Lösung

$\Rightarrow x' = 6$

2)

$[2^{427}]_7 = [2]_7^{427} \underset{MR}{=} [2]_7^{[427]_3} = [2]_7^{[1]_3} = [2]_7$

$\Rightarrow$ Rest 2

NR:

- in $\mathbb{Z}/7\mathbb{Z}$ gilt: $1 \xrightarrow{\cdot 2} 2 \xrightarrow{\cdot 2} 4 \xrightarrow{\cdot 2} 1$ (= 8)

  $\Rightarrow ord(2) = 3$ in $\mathbb{Z}/7\mathbb{Z}$

- $[427]_3 = [1]_3$ via Division mit Rest (TR)

3)

Alternativ mit Eulerschen Satz (Satz 5.24):

$ggT(2, 7) = 1$ und $\varphi(7) = 6$ ($= 7-1$, da 7 prim)

$\Rightarrow [2^{427}]_7 = [2]_7^{[427]_6} \overset{TR}{=} [2]_7^{[1]_6} = [2]_7$

3)

$$\begin{aligned} x &\equiv 3 \pmod 5 \\ x &\equiv 1 \pmod 7 \\ x &\equiv 2 \pmod{11} \end{aligned} \quad \Rightarrow \quad \left\{ \begin{array}{ll} a_1 = 3, & m_1 = 5 \\ a_2 = 1, & m_2 = 7 \\ a_3 = 2, & m_3 = 11 \end{array} \right\}$$

m_i paarweise teilerfremd $\Rightarrow$ Chinesischer Restsatz anwendbar

Konstruiere $x := a_1 q_1 q_1' + a_2 q_2 q_2' + a_3 q_3 q_3'$

mit

- $q_1 := m_2 \cdot m_3 = 77, \quad \overline{q_1} = \overline{2}$ (in $\mathbb{Z}/5\mathbb{Z}$)
  $\overline{q_1}^{-1} = \overline{3}$
  $\Rightarrow$ wähle $q_1' := 3$

- $q_2 := m_1 \cdot m_3 = 55, \quad \overline{q_2} = \overline{6}$ (in $\mathbb{Z}/7\mathbb{Z}$)
  $\overline{q_2}^{-1} = \overline{6}$
  $\Rightarrow$ wähle $q_2' := 6$

- $q_3 := m_1 \cdot m_2 = 35, \quad \overline{q_3} = \overline{2}$ (in $\mathbb{Z}/11\mathbb{Z}$)
  $\overline{q_3}^{-1} = \overline{6}$
  $\Rightarrow$ wähle $q_3' := 6$

D.h. $x = 3 \cdot 77 \cdot 3 + 1 \cdot 55 \cdot 6 + 2 \cdot 35 \cdot 6 = 1443$

Kanonischer Repräsentant für Lösung ist kanonischer Repräsentant für 1443 in $\mathbb{Z}/m\mathbb{Z}$, $m = m_1 \cdot m_2 \cdot m_3 = 385$:

$x_{\text{kanonisch}} = 288$ (mit TR)

Probe (mit TR) ✓

4.) Repräsentiere Ziffern zur Basis 12 mit $\{0, \dots, 9, A, B\}$.

(1) $BB21_{12} = 11 \cdot 10^3 + 11 \cdot 10^2 + 2 \cdot 10^1 + 1 \cdot 10^0$

$= 11000 + 1100 + 20 + 1$

$= 12221_{10}$

(2) $50AB_{12} = 5 \cdot 10^3 + 0 \cdot 10^2 + 10 \cdot 10^1 + 11 \cdot 10^0$

$= 5000 + 10 + 11$

$= 5021_{10}$.