# Übungsblatt № 11

## Aufgabe 70: Euklidischer Algorithmus

a) Wenden Sie den euklidischen Algorithmus an um ggT$(65, 77)$ zu berechnen
b) Bestimmen Sie alle $x \in \mathbb{Z}$ mit

$$x \equiv 2 \mod 77 \qquad x \equiv 7 \mod 65$$

Zu a):

$$\begin{aligned}77 &= 1 \cdot 65 + 12\\ 65 &= 5 \cdot 12 + 5\\ 12 &= 2 \cdot 5 + 2\\ 2 &= 1 \cdot 1 + 0\end{aligned}$$

Somit ist ggT$(65, 77)$.

Zu b): Wir verwenden den chinesischen Restsatz.

**Satz 1** (Chinesischer Restsatz)**.** *Seien $b_1, \dots, b_k$ und $m_1, \dots, m_k$ natürliche Zahlen, und* ggT$(m_i, m_j) = 1$ *für $1 \leq i < j \leq k$, dann gibt es für $m = m_1 \cdot \dots \cdot m_k$ genau ein $x \in \mathbb{Z}/m\mathbb{Z}$ mit*

$$\forall i \in [k] \colon x = [b_i]_{m_i}$$

Wir führen noch die Notation $[x^{-1}]_k$ ein. Diese Restklasse beschreibt das inverse Element zu $[x]_k$ bezüglich der Multiplikation in $\mathbb{Z}/k\mathbb{Z}$, sprich $[x^{-1}]_k \cdot [x]_k = [1]_k$. Hier ist es wichtig anzumerken, dass $\mathbb{Z}/k\mathbb{Z}$ nur für $k$ prim ein Körper ist und alle $[x^{-1}]_k$ existieren.

Sei $k \in [65^{-1}]_{77}$ und $l \in [77^{-1}]_{65}$:

$$\begin{aligned}x &= 2 \cdot 65 \cdot k + 7 \cdot 77 \cdot l\\ [x]_{65} &= [539]_{65} \cdot [77^{-1}]_{65}\end{aligned}$$

Wir lösen noch $[y]_{65}[77]_{65} = [1]_{65}$. Dazu verwenden wir $[77]_{65} = [12]_{65}$:

$$[12y]_{65} = [1]_{65}1$$

## Aufgabe 73

Beweisen Sie, dass $n^5 - n \equiv 0 \mod 30$.

Wir faktorisieren $n^5 - n = (n-1)n(n+1)(n^2+1)$. Offensichtlich ist einer der Faktoren $n-1$, $n$ oder $n+1$ durch drei teilbar. Des weiteren ist entweder $n$ gerade oder $n+1$ und $n-1$. Damit gilt $6 \mid n^5 - n$. Ist $n$ ein Vielfaches von 5 so folgt die Behauptung. Für $n \equiv 1 \mod 5$ ist $n-1$ ein Vielfaches von 5. Im Fall $n \equiv 4 \mod 5$ ist $n+1$ ein Vielfaches von 5. Es bleiben die Fälle $n \equiv 2 \mod 5$ und $n \equiv 3 \mod 5$:

$$\begin{aligned}n \equiv 2 \mod 5 &\implies \exists k \in \mathbb{N} \colon n = 5k+2 \implies n^2 + 1 = 25k^2 + 20k + 4 + 1 = 25k^2 + 20k + 5 \equiv 0 \mod 5\\ n \equiv 3 \mod 5 &\implies \exists k \in \mathbb{N} \colon n = 5k+3 \implies n^2 + 1 = 25k^2 + 30k + 9 + 1 = 25k^2 + 30k + 10 \equiv 0 \mod 5\end{aligned}$$

Damit haben wir also immer die Teiler $2, 3, 5$ in $n^5 - n$ womit auch 30 ein Teiler von $n^5 - n$ ist.