Lösungen zu den Übungsaufgaben

Diskrete Mathematik

WS 04/05

Blatt 6

Aufgabe 6.1

$x \equiv 310643 \pmod{654321}$

Aufgabe 6.2

$x \equiv 95923 \pmod{367200}$

Aufgabe 6.3

In $\mathbb{Z}_{10}$ gilt: $14^{72} \equiv 4^{72} \pmod{10}$.

Wir sehen schnell, dass $4^2 = 16 \equiv 6 \pmod{10}$ und $4^3 = 4 \cdot 4^2 \equiv 4 \cdot 6 = 24 \equiv 4 \pmod{10}$. Damit gilt für alle $n \in \mathbb{N}$:

$$4^n \equiv \begin{cases} 4 & \text{wenn } n \text{ ungerade} \\ 6 & \text{wenn } n \text{ gerade} \end{cases} \pmod{10}$$

Damit ist $14^{72} \equiv 6 \pmod{10}$.

Aufgabe 6.4

Behauptung :

$$\mathbb{Z}_m^* = \{\ a \in \mathbb{Z}_m \mid \mathrm{ggT}(a, m) = 1\}$$

Beweis :

$\subseteq$: Nach Satz 3.12 berechnet der erweiterte Euklidische Algorithmus zwei Zahlen $x, y \in \mathbb{Z}$, so dass gilt $mx + ay = \mathrm{ggT}(a, m) = 1$. Damit folgt

$$mx = 1 - ay \Leftrightarrow 1 \equiv ay \equiv ya \pmod{m} \ .$$

y ist folglich inverses Element zu a und damit $a \in \mathbb{Z}_m^*$.

$\supseteq$: Wir zeigen $\mathrm{ggT}(a, m) > 1 \Rightarrow a \notin \mathbb{Z}_m^*$.
Sei $\mathrm{ggT}(a, m) =: d > 1$, dann existieren $b, c \in \mathbb{Z} \setminus \{0\}$, so dass $bd = a$ und $cd = m$. Damit gilt aber:

$$ac = (bd)c = b(cd) = bm \equiv 0 \pmod{m} \ .$$

Wir nehmen nun an, dass zu a ein inverses Element $a^{-1} \in \mathbb{Z}_m$ existiert. Dann gilt

$$0 \equiv a^{-1}(ac) = (a^{-1}a)c \equiv c \pmod{m} \ .$$

Dies widerspricht der Annahme, dass $c \neq 0$. Folglich gilt $a \notin \mathbb{Z}_m^*$.