S. Wewers, S. Wilke

Kryptographie, SS 06

# Lösung 4

**Aufgabe 1.**
Ansatz: $x \equiv a \cdot 3 \cdot 5 + b \cdot 3 \cdot 7 + c \cdot 5 \cdot 7 \pmod{3 \cdot 5 \cdot 7 = 105}$.
Dies führt zu den Gleichungen:

$$\begin{aligned} x \equiv 3 \cdot 5 \cdot a \equiv 15 \cdot a \equiv a &\overset{!}{\equiv} 2 \pmod 7 \\ x \equiv 3 \cdot 7 \cdot b \equiv 21 \cdot b \equiv b &\overset{!}{\equiv} 3 \pmod 5 \\ x \equiv 5 \cdot 7 \cdot c \equiv 35 \cdot c \equiv 2 \cdot c &\overset{!}{\equiv} 2 \pmod 3 \end{aligned}$$

Damit folgt $a = 2$, $b = 3$, $c = 1$, also $x = 30 + 63 + 35 = 128 \equiv 23 \pmod{105}$.
Die kleinste positive Lösung ist also: 23.

**Aufgabe 2.**

(a) Es gilt: $3, 4, 5, 6 \mid (x + 1)$, also auch $\text{kgV}(3, 4, 5, 6) = 60 \mid (x + 1)$ bzw. $x \equiv -1 \equiv 59 \pmod{60}$.

(b) Ansatz:

$$\begin{aligned} x &\equiv 2 \pmod 3 & a_1 &= 2 & M_1 &= 5 \cdot 2 = 10 \\ x &\equiv 1 \pmod 5 & a_2 &= 1 & M_2 &= 2 \cdot 3 = 6 \\ x &\equiv 5 \equiv 1 \pmod 2 & a_3 &= 5 & M_3 &= 3 \cdot 5 = 15 \end{aligned}$$

Bestimmung der Inversen zu $M_i$:

$$\begin{aligned} 1 &\overset{!}{\equiv} 10 \cdot \overline{M}_1 \equiv 1 \cdot \overline{M}_1 \pmod 3 &&\Rightarrow \overline{M}_1 = 1 \\ 1 &\overset{!}{\equiv} 6 \cdot \overline{M}_2 \equiv 1 \cdot \overline{M}_2 \pmod 5 &&\Rightarrow \overline{M}_2 = 1 \\ 1 &\overset{!}{\equiv} 15 \cdot \overline{M}_3 \equiv 1 \cdot \overline{M}_3 \pmod 2 &&\Rightarrow \overline{M}_3 = 1 \end{aligned}$$

Damit ist

$$\begin{aligned} x &\equiv a_1 M_1 \overline{M}_1 + a_2 M_2 \overline{M}_2 + a_3 M_3 \overline{M}_3 \\ &\equiv 2 \cdot 10 \cdot 1 + 1 \cdot 6 \cdot 1 + 5 \cdot 15 \cdot 1 \\ &\equiv 20 + 6 + 15 \equiv 41 \equiv 11 \pmod{30} \end{aligned}$$

**Aufgabe 3.**
Es ist $17^x \equiv -2 \pmod{35} \Leftrightarrow 17^x \equiv -2 \pmod 5$ und $17^x \equiv -2 \pmod 7$.
Es ist $17^x \equiv 2^x \overset{!}{\equiv} -2 \equiv 3 \pmod 5$. Wegen $2^3 = 8 \equiv 3 \pmod 5$ folgt damit $x \equiv 3 \equiv -1 \pmod{\phi(5) = 4}$.

Weiter ist $17^x \equiv 3^x \stackrel{!}{\equiv} -2 \equiv 5 \pmod 7$. Wegen $3^2 \equiv 9 \equiv 2 \pmod 7$ und $3^3 \equiv 27 \equiv -1 \pmod 7$ folgt $3^5 \equiv -2 \pmod 7$, also $x \equiv 5 \equiv -1 \pmod{\phi(7) = 6}$. Insgesamt folgt $x \equiv -1 \pmod{\text{kgV}(4,6) = 12}$, also $x \equiv 11 \pmod{12}$.

Alternativlösung: Bestimme zunächst $y \in \mathbb{N}$ mit $(-2)^y \equiv 17 \pmod{35}$. Die Potenzen von $(-2)$ berechnen sich schnell wie folgt: $(-2)^1 \equiv -2$, $(-2)^4 \equiv 4$, $(-2)^3 \equiv 8$, $(-2)^4 \equiv 16$, $(-2)^5 \equiv 3$, $(-2)^6 \equiv -6$, $(-2)^7 \equiv 12$, $(-2)^8 \equiv 11$, $(-2)^9 \equiv 13$, $(-2)^{10} \equiv 9$, $(-2)^{11} \equiv 17$. Daraus folgt

$$17^x \equiv ((-2)^{11})^x \equiv (-2)^{11x} \stackrel{!}{\equiv} -2 \pmod{35}$$

Nun ist $\phi(35) = 24$, und daher gilt $(-2)^{24} \equiv 1 \pmod{35}$. Daraus folgt nun $11x \equiv 1 \pmod{24}$. Wegen $11 \cdot 11 = 121 \equiv 1 \pmod{24}$ folgt daher $x \equiv 11 \pmod{24}$.

Bemerkung: Beim zweiten Lösungsansatz bekommt man zunächst nur die Hälfte der Lösungen. Dies liegt daran, dass bereits $(-2)^{12} = 4096 \equiv 1 \pmod{35}$. Daraus erhält man analog die Gleichung $11x \equiv 1 \pmod{12}$, die sich zu $x \equiv 11 \pmod{12}$ lösen lässt.

**Aufgabe 4.**

(a) Es ist $f(\alpha+1) = (\alpha+1)^2 + (\alpha+1) + 1 = \alpha^2 + 2\alpha + 1 + \alpha + 1 + 1 = \alpha^2 + \alpha + 1 = f(\alpha) = 0$.

(b) Die Bedingungen für $i = 1, 2$ liefern das lineare Gleichungssystem:

$$\left(\begin{array}{cc|c} 1 & 1 & 1 \\ \alpha & \alpha+1 & 1 \end{array}\right) \rightsquigarrow \left(\begin{array}{cc|c} 1 & 1 & 1 \\ 0 & 1 & 1+\alpha \end{array}\right) \rightsquigarrow \left(\begin{array}{cc|c} 1 & 0 & \alpha \\ 0 & 1 & 1+\alpha \end{array}\right)$$

Also gilt: $c_1 = \alpha$, $c_2 = 1 + \alpha$. Zur Kontrolle:

$$\begin{aligned}
c_1 \cdot 1 + c_2 \cdot 1 &= \alpha + (1+\alpha) = 1 = a_0 \\
c_1 \cdot \alpha + c_2 \cdot (1+\alpha) &= \alpha^2 + (\alpha^2 + 1) = 1 = a_1 \\
c_1 \cdot \alpha^2 + c_2 \cdot (1+\alpha)^2 &= \alpha^3 + \alpha^3 + \alpha^2 + \alpha + 1 = \alpha^2 + \alpha + 1 = 0 = a_2 = a_1 + a_0 \\
c_1 \cdot \alpha^3 + c_2 \cdot (1+\alpha)^3 &= \alpha^4 + 1 + \alpha^4 = 1 = a_3 = a_2 + a_1 \\
c_1 \cdot \alpha^4 + c_2 \cdot (1+\alpha)^4 &= \alpha^5 + 1 + \alpha + \alpha^4 + \alpha^5 = 1 + \alpha + \alpha^4 = 1 + \alpha + (\alpha+1)^2 \\
&= 1 + \alpha + 1 + \alpha^2 = \alpha + \alpha^2 = 1 = a_4 = a_3 + a_2
\end{aligned}$$

Erklärung: Die Folge $a_i$ lässt sich wie folgt beschreiben:

$$\begin{pmatrix} a_{n+1} \\ a_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a_n \\ a_{n-1} \end{pmatrix} = \cdots = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \cdot \begin{pmatrix} a_1 \\ a_0 \end{pmatrix}$$

Die Matrix $A := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ hat als charakteristisches Polynom $X \cdot (X+1) + 1 = X^2 + X + 1 = f(X)$. Die Eigenwerte von $A$ sind also gerade

$\alpha+1, \alpha$ als Nullstellen von $f$. Als zugehörige Eigenvektoren findet man $(1, \alpha)$ bzw. $(1, \alpha+1)$; $A$ hat also die Gestalt:

$$A = \begin{pmatrix} 1 & 1 \\ \alpha & 1+\alpha \end{pmatrix} \cdot \begin{pmatrix} \alpha+1 & 0 \\ 0 & \alpha \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ \alpha & 1+\alpha \end{pmatrix}^{-1}$$

Als Inverse erhält man $\begin{pmatrix} 1+\alpha & 1 \\ \alpha & 1 \end{pmatrix}$, und daher gilt:

$$\begin{aligned} \begin{pmatrix} a_{n+1} \\ a_n \end{pmatrix} &= \begin{pmatrix} 1 & 1 \\ \alpha & 1+\alpha \end{pmatrix} \cdot \begin{pmatrix} (\alpha+1)^n & 0 \\ 0 & \alpha^n \end{pmatrix} \cdot \begin{pmatrix} 1+\alpha & 1 \\ \alpha & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 \\ \alpha & 1+\alpha \end{pmatrix} \cdot \begin{pmatrix} (\alpha+1)^n \cdot \alpha \\ \alpha^n \cdot (1+\alpha) \end{pmatrix} = \begin{pmatrix} (\alpha+1)^n \cdot \alpha + \alpha^n \cdot (1+\alpha) \\ (\alpha+1)^n \cdot \alpha^2 + \alpha^n \cdot (1+\alpha)^2 \end{pmatrix} \\ &= \begin{pmatrix} (\alpha+1)^n \cdot \alpha + \alpha^n \cdot (1+\alpha) \\ (\alpha+1)^n \cdot \alpha^2 + \alpha^n \cdot (1+\alpha)^2 \end{pmatrix} = \begin{pmatrix} (\alpha+1)^{n+1} \cdot (\alpha+1) + \alpha^{n+1} \cdot \alpha \\ (\alpha+1)^n \cdot (\alpha+1) + \alpha^n \cdot \alpha \end{pmatrix} \end{aligned}$$

Daraus folgt nun ebenfalls $c_1 = \alpha$, $c_2 = \alpha + 1$.