Übung 32

(a) **Aufgabe:**
Bestimmen sie $f \circ g$.
Lösung:
$f \circ g : \mathbb{Z} \to \{1, 2, 3, ..., p-1\}, x \mapsto 10$, wenn $\exists y \in \mathbb{N} : x = 3 * y + 1$, sonst 1

(b) **Aufgabe:**
Geben sie den Wertebereich an, sodass die Funktion surjektiv ist.
Lösung:
Eine Funktion ist surjektiv, wenn jedes Element des Wertebereichs ein nicht leeres Urbild hat.
Das Bild einer Zahl, für die $\exists y \in \mathbb{N} : x = 3 * y + 1$ gilt, ist immer 10, da wenn g auf diese Zahl angewendet wird, als Bild von g 10 weiter an f gegeben wird und 2^{10} *mod* $13 = 10$ gilt.
Das Bild jeder anderen Zahl ist 1, da wenn eine Zahl durch 3 teilbar ist, das Bild über g als 0 weitergegeben wird und $2^0 = 1$, und da für jede andere Zahl 12 weitergegeben wird und 2^{12} *mod* $13 = 1$ gilt.
Dementsprechend ist $\{1, 10\}$ der Wertebereich, der die Funktion surjektiv macht.

(c) **Aufgabe:**
Bestimmen sie $g \circ f$.
Lösung:

$$g \circ f : \{0, 2, 3, ..., p-1\} \to \{0, 2, 3, ..., p-1\}, x \mapsto \begin{cases} 0, & \text{wenn } 3 \mid (a^x \mod p) \\ 10, & \text{wenn } \exists y \in \mathbb{N} : a^x = 3 \cdot y + 1 \mod p \\ 12, & \text{sonst} \end{cases}$$

(d) **Aufgabe:**
Bestimmen sie $(g \circ f)^{-1}(0)$.
Lösung:
$(g \circ f)^{-1}(0) = \{4, 5, 6, 8\}$

(e) **Aufgabe:**
Warum ist der Vorschlag für die Verschlüsselung ungeeignet?
Lösung:
Wenn man die neue Funktion $g \circ (f \circ g)$ auf eine beliebige ganze Zahl anwendet, muss zuerst $(f \circ g)$ und danach noch g angewendet werden. Wie in (b) erklärt ist das Bild für beliebige ganze Zahlen, auf die die Funktion angewendet werden soll, Element aus $\{1, 10\}$, also 1 oder 10. Wendet man g auf 1 an, so ist die Bedingung $\exists y \in \mathbb{N} : x = 3 * y + 1$ erfüllt, da $1 = 3 * 0 + 1$ gilt. Das Bild ist also 10. Wendet man g auf 10 an, so ist die Bedingung $\exists y \in \mathbb{N} : x = 3 * y + 1$ erfüllt, da $10 = 3 * 3 + 1$ gilt. Das Bild ist auch also 10. Die Funktion $g \circ (f \circ g)$ bildet jede ganze Zahl also auf 10 ab. Da sich die Gesprächspartner anhand des Bilds authentifizieren wollen, ist das vorgeschlagene Verfahren ungeeignet.