Prof. Buchholz, Diskrete Strukturen SoSe 2009, Zweitklausur (2. November 2009) Aufgabe 3: *Man bestimme* $n \in \{0, \ldots, 76\}$*, so daß* $n^{37} \equiv 2 \bmod 77$. (Erläuterung der Musterlösung, Uwe Lück 4. Januar 2010:)

77 ist Produkt der Primzahlen 7 und 11. Als solche (und weil verschieden) sind sie *teilerfremd*. Für die *Euler-Funktion* φ folgt mit *Lemma 4.5* und *Korollar 1* von S. 17 des Skriptums $\varphi(77) = \varphi(7) \cdot \varphi(11) = 6 \cdot 10 = 60$.

Der *Euklidische Algorithmus* liefert nach *Lemma 3.4* $\mathsf{ggt}(\varphi(77), 37) = 1 = -8 \cdot \varphi(77) + 13 \cdot 37$, also

$$13 \cdot 37 \equiv 1 \bmod \varphi(77) \qquad (*)$$

Ansonsten beruht die Lösung der Aufgabe auf *Lemma 4.9* des Skriptums. (Die Nachricht 2 wird mit dem zum *privaten Schlüssel* $(77, 37)$ gehörigen *öffentlichen Schlüssel* $(77, 13)$ gemäß *RSA-Verfahren* kodiert.)

$\mathbb{Z}_{77}$ ist $\{0, \ldots, 76\}$, und für $s \in \mathbb{N}$ ist $V_s \colon \mathbb{Z}_{77} \to \mathbb{Z}_{77}$ durch $V_s(x) = \mathbf{r}_{77}(x^s)$ definiert. Wegen $(*)$ folgt $V_{37}(V_{13}(2)) \equiv 2 \bmod 77$. Nach Definition von V_{13} und V_{37} erfüllt

$$n := V_{13}(2) = 30$$

also die Bedingungen $n \in \mathbb{Z}_{77}$ und $n^{37} \equiv 2 \bmod 77$ der Aufgabenstellung.

Das genügt eigentlich bereits als Lösung der Aufgabe. Tatsächlich ist aber $V_{37} \circ V_{13}$ nach L. 4.9 surjektiv, damit ist auch V_{37} surjektiv und nach L. 2.5 (Definitions- und Wertebereich von gleicher endlicher Mächtigkeit) auch *injektiv*. Daher ist $V_{13}(2)$ sogar das *einzige* $n \in \mathbb{Z}_{77}$, das $n^{37} \equiv 2 \bmod 77$ erfüllt.

($x \mapsto \mathbf{r}_m(x^s)$ ist *nicht allgemein* injektiv auf $\mathbb{Z}_m$, z. B. $\mathbf{r}_6(2^2) = 4 = \mathbf{r}_6(4^2)$.)