Aufgabe F20T3A2

Berechnen Sie die letzten beiden Ziffern der Zahl

$$2018^{(2019^{2020})}.$$

Gehen Sie dazu wie folgt vor:

(a) Berechnen Sie die Klasse von $2018^{(2019^{2020})}$ in $\mathbb{Z}/25\mathbb{Z}$.

(b) Zeigen Sie, dass $[2018^{(2019^{2020})}] = 0$ in $\mathbb{Z}/4\mathbb{Z}$ gilt.

(c) Schließen Sie die Berechnung mit Hilfe des Chinesischen Restsatzes ab.

Lösung:

zu (a) Laut Vorlesung gilt $|\mathbb{Z}/25\mathbb{Z}^\times| = \varphi(25) = 20$, und in $\mathbb{Z}/20\mathbb{Z}^\times$ gilt

$$[2019]^{2020} = [19]^{2020} = [-1]^{2020} = ([-1]^2)^{1010} = [1]^{1010} = 1.$$

Es folgt $2019^{2020} \equiv 1 \bmod 20$; es existiert also ein $k \in \mathbb{Z}$ mit $2019^{2020} = 1 + 20k$. Wegen $|\mathbb{Z}/25\mathbb{Z}^\times| = 20$ gilt $\bar{c}^{20} = \bar{1}$ für alle $\bar{c} \in (\mathbb{Z}/25\mathbb{Z})^\times$. Wegen $5 \nmid 2018$ folgt $\mathrm{ggT}(2018, 25) = 1$, also ist die Klasse $[2018]$ von 2018 in $\mathbb{Z}/25\mathbb{Z}$ in $(\mathbb{Z}/25\mathbb{Z})^\times$ enthalten. Daraus wiederum folgt

$$[2018^{(2019^{2020})}] = [2018^{1+20k}] = [2018] \cdot ([2018]^{20})^k = [2018] \cdot [1]^k = [2018] = [18].$$

zu (b) Für alle $k \geq 2$ gilt $4 \mid 2^k$ und somit $[2]^k = [0]$ in $\mathbb{Z}/4\mathbb{Z}$, und es ist $2019^{2020} \geq 2019 \geq 2$. Wegen $2018 \equiv 2 \bmod 4$ folgt $[2018]^{(2019^2 020)} = [2]^{(2019^{2020})} = [0]$ in $\mathbb{Z}/4\mathbb{Z}$.

zu (c) Laut Chinesischem Restsatz existiert ein (eindeutig bestimmter) Ringhisomorphismus $\phi : \mathbb{Z}/100\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$ mit $\phi(c + 100\mathbb{Z}) = (c + 4\mathbb{Z}, c + 25\mathbb{Z})$ für alle $c \in \mathbb{Z}$. Daraus folgt: Sind $c_1, c_2 \in \mathbb{Z}$ mit $c_1 \equiv c_2 \bmod 4$ und $c_1 \equiv c_2 \equiv c_2 \bmod 25$, dann folgt $c_1 \equiv c_2 \bmod 100$. Denn auf Grund der Voraussetzung gilt

$$\phi(c_1 + 100\mathbb{Z}) = (c_1 + 4\mathbb{Z}, c_1 + 25\mathbb{Z}) = (c_2 + 4\mathbb{Z}, c_2 + 25\mathbb{Z}) = \phi(c_2 + 100\mathbb{Z}).$$

Aus der Injektivität von ϕ folgt $c_1 + 100\mathbb{Z} = c_2 + 100\mathbb{Z}$, und dies wiederum ist gleichbedeutend mit $c_1 \equiv c_2 \bmod 100$.

Es gibt gibt genau vier Zahlen $c \in \mathbb{Z}$ mit $0 \leq c < 100$ mit $c \equiv 18 \bmod 25$, nämlich 18, 43, 68 und 93. Nur eine dieser Zahlen erfüllt auch die Bedingung $c \equiv 0 \bmod 4$, nämlich 68. Sei nun $c_1 = 2018^{(2019^{2020})}$ und $c_2 = 68$. Nach Teil (a) gilt $c_1 \equiv 18 \equiv 68 \equiv c_2 \bmod 25$, und nach Teil (b) gilt $c_1 \equiv 0 \equiv 68 \equiv c_2 \bmod 4$. Wie soeben ausgeführt, folgt daraus $c_1 \equiv c_2 \bmod 100$, also $c_1 \equiv 68 \bmod 100$. Dies bedeutet, dass die letzten beiden Ziffern der Zahl c_1 durch 6 und 8 gegeben sind.