

$$\overline{a}^x \equiv \overline{b} \pmod{\overline{p}}$$

$$p-1=40=2^3 \cdot 5$$

$$p-m \quad q=2, \quad \alpha=3$$

$$x_0: 7^{20x_0} \equiv 25^{20} \equiv 1 \Rightarrow x_0 = 0$$

$$b_1 = 25 \cdot 7^{-0 \cdot 2^0} = 25$$

$$x_1: 7^{20x_1} \equiv 25^{40/4} \equiv 25^{10} \equiv 1 \Rightarrow x_1 = 0$$

$$b_2 = 25 \cdot 7^{-0 \cdot 2^1} = 25$$

$$x_2: 7^{20x_2} \equiv 25^{40/8} \equiv 25^5 \equiv 40 \Rightarrow x_2 = 1$$

$$\Rightarrow x \equiv 0 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2 \pmod{8} \equiv \boxed{4 \pmod{8}}$$

$$p-m \quad q=5, \quad \alpha=1$$

$$x_0: 7^{8x_0} \equiv 25^8 \equiv 37 \Rightarrow x_0 = 1$$

$$\Rightarrow x \equiv x_0 \cdot 5^0 \equiv 1 \cdot 5^0 \equiv \boxed{1 \pmod{5}}$$

$$\Rightarrow \begin{cases} x \equiv 4 \pmod{8} \\ x \equiv 1 \pmod{5} \end{cases} \Rightarrow x \equiv 36 \pmod{41}$$

$$\text{Antwort: } x = 36$$

$$b \frac{p-1}{q} \equiv a \frac{p-1}{q} \cdot x_0 \pmod{p}$$

$$b_i = b_{i-1} \cdot a^{-x_{i-1} \cdot q^{i-1}}$$

$$\left(a \frac{p-1}{q}\right)^{x_i} \equiv b_i \frac{p-1}{q^{i+1}}$$

i	0	1	2	3
2^i	1	2	4	8
5^i	1	5	25	125